

Der Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr

DISSERTATION

der Rechts- und staatswissenschaftlichen Fakultät
der Universität Zürich
zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

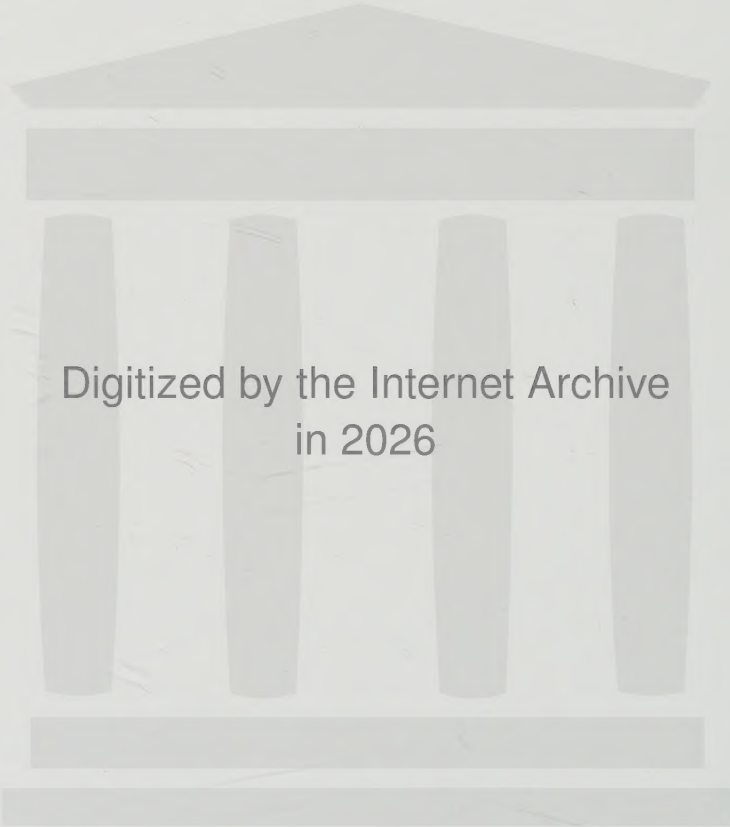
LUCIUS N. WOCHNER

von Eggersriet-Grub SG

genehmigt auf Antrag von

Herrn Prof. Dr. Peter Forstmoser

1981



Digitized by the Internet Archive
in 2026

Der Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr

DISSERTATION

der Rechts- und staatswissenschaftlichen Fakultät
der Universität Zürich
zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

LUCIUS N. WOCHNER

von Eggersriet-Grub SG

genehmigt auf Antrag von

Herrn Prof. Dr. Peter Forstmoser

Schulthess Polygraphischer Verlag AG, Zürich

Die Rechts- und staatswissenschaftliche Fakultät gestattet hierdurch die Drucklegung vorliegender Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 27. Mai 1981

Der Dekan:
Prof. Dr. Gerold Hauser



Die gleiche Arbeit ist im Schulthess Polygraphischer Verlag AG, Zürich, erschienen als Heft 11 der Reihe

Computer und Recht

Herausgegeben von: Prof. Dr. K. Bauknecht, Prof. Dr. P. Forstmoser, Prof. Dr. C.A. Zehnder

© Schulthess Polygraphischer Verlag AG, Zürich 1981
ISBN 3 7255 2158 1

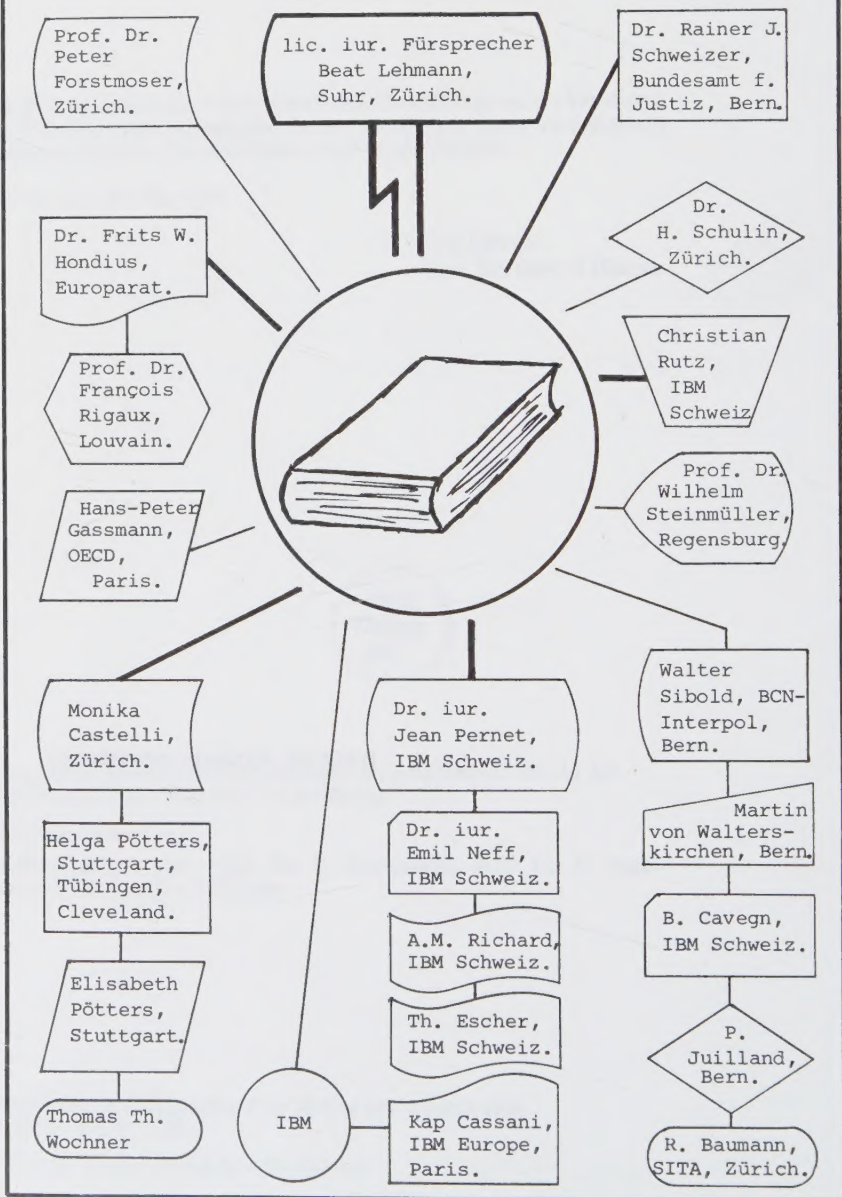
Druck: Huber Druck AG, Entlebuch

THANKSGIVING BOARD



Meinen Eltern gewidmet.

THANKSGIVING BOARD



VORWORT

Anstoss zur vorliegenden Arbeit gab mir meine Tätigkeit als Werkstudent bei der Firma IBM Schweiz während meines Studiums. Nachdem ich mich 1975 erstmals im Rahmen einer Seminararbeit anlässlich des von Prof. P. Forstmoser an der Universität Zürich geführten Seminars "Computer und Recht" mit dem Thema des grenzüberschreitenden Datenverkehrs auseinandergesetzt und Prof. P. Forstmoser anfangs 1978 das vorliegende Dissertationsthema angenommen hatte, konnte ich meine Werkstudententätigkeit bei der IBM bis zum Ende der Doktorarbeit im September 1980 fortsetzen. Ich hatte während dieser Zeit nicht nur Gelegenheit, die dem Juristen oft (noch) fremde Welt des Computers tiefer kennenzulernen, sondern auch die Möglichkeit der direkten Anwendung, sei es im Rahmen meiner Tätigkeit als Werkstudent, sei es im Zusammenhang mit den Arbeiten an meiner Dissertation. Ohne diesen tiefen Einblick in die Welt der Informatik und ohne das mir ebenfalls von IBM gewährte "Einsichtsrecht" in die juristische Dokumentation zum Datenschutz, wäre diese Arbeit wohl kaum zustandegekommen.

Ich hoffe, dass die direkte Begegnung mit der EDV ihren Niederschlag in Form von pragmatischen und nicht rein dogmatischen Lösungsansätzen gefunden hat.

An dieser Stelle sei der Firma IBM Schweiz mein herzlichster Dank ausgesprochen.

Wie erwähnt, wurde die Arbeit anfangs 1978 in Angriff genommen und Ende September 1980 fertiggestellt.¹ Ich war während dieser Zeitspanne nicht nur mit dem Problem der rasanten Entwicklung auf dem Gebiet der Computer- und Kommunikationstechnologie konfrontiert, sondern stand auch im Sog der neuesten rechtlichen Entwicklungen im Bereich des Datenschutzes auf nationaler und vor allem auf internationaler Ebene. So hatte ich z.B. meine Ausführungen über die Datennetze SITA, SWIFT, INTERPOL und EURONET (vgl. hinten § 8) bereits abgeschlossen, als die OECD Publikation "Utilisation des réseaux internationaux de transmission des données en Europe" erschien. Glück-

licherweise konnten kurz vor Beendigung des Manuskripts der Europarat und die OECD ihre im Entwurf vorliegenden Vereinbarungen zum grenzüberschreitenden Datenverkehr verabschieden, so dass sie in dieser Arbeit in ihrer definitiven Fassung berücksichtigt werden konnten. Für die Betrachtungen zu diesen internationalen Vereinbarungen standen mir aber weder umfangreiche Literatur noch grössere, praktische Erfahrung hinsichtlich ihrer Anwendung zur Verfügung.

-
- 1 Die Literatur wurde bis Ende Dezember 1980 berücksichtigt.
 - 2 Hierzu erfolgten noch vor Drucklegung einige Nachführungen.

INHALTSUEBERSICHT

Die vorliegende Arbeit ist in drei Teile gegliedert. Der erste Teil skizziert die im Zusammenhang mit dem grenzüberschreitenden Datenverkehr auftauchenden Fragen und Probleme. Er verschafft eine Einführung und einen Einblick in die komplexen Zusammenhänge und die aus dem Datentransfer resultierenden Problemkreise.

Hier wird vorab die Notwendigkeit des grenzüberschreitenden Datenverkehrs bei der Aufgabenerfüllung der Wirtschaft und Verwaltung nachgewiesen (§ 1) und die durch die Uebermittlung verursachten Probleme des Persönlichkeitsschutzes aufgezeigt (§ 2). Zusätzlich werden nicht juristische Probleme, die wirtschaftliche und politische Aspekte betreffen, summarisch dargestellt (§§ 3 und 4). Einen weiteren, zugleich zentralen Problemkreis des grenzüberschreitenden Datenverkehrs stellen die gegensätzlichen Interessen des Datenschutzes und der Informationsfreiheit als Ausfluss des Postulats nach einem freien Datenfluss dar (§ 5). Im Verhältnis von Datenschutz-bewussten Nationen und solchen ohne Datenschutzbestimmungen gilt es, die Lücken zu schließen, die aus der Ungleichheit des Schutzvermögens der Persönlichkeit resultieren, um einen effizienten Datenschutz zu erreichen. Hier erfolgt eine Darstellung des Problems (§ 6). Der Umfang dieser Arbeit ist beschränkt, so dass nur die markantesten Problemkreise, die durch die grenzüberschreitende Uebermittlung personenbezogener Daten auftauchen, im Hinblick auf mögliche Lösungsansätze (vgl. 3. Teil) besprochen werden können.

Der zweite Teil bringt eine Darstellung des grenzüberschreitenden Datenverkehrs. Inhaltlich ist er in zwei Abschnitte gegliedert: Einerseits wird der grenzüberschreitende Datenverkehr in seinen hauptsächlichsten Erscheinungsformen beschrieben und andererseits ein Ueberblick über die existierenden rechtlichen Regelungen einzelner Länder Europas sowie über die neuesten internationalen Vereinbarungen zum transnationalen Datenaustausch gegeben.

Bevor auf die Erscheinungsformen des grenzüberschreitenden Datenverkehrs näher eingegangen wird, erfolgt zunächst eine technische Begriffsbestimmung des grenzüberschreitenden Verkehrs, die für das Ver-

ständnis der nachfolgenden Ausführungen notwendig ist (§ 7). In § 8 werden die Datennetze als charakteristische Medien des transnationalen Datenflusses typisiert. Da auf diesen Netzen zur Zeit der grösste Teil des internationalen Informationsverkehrs stattfindet, werden einzelne Träger solcher Datennetze aus verschiedenen Bereichen und die damit verwirklichten Anwendungen zum besseren Verständnis der Vorgänge beschrieben sowie andere mögliche Formen und Medien der Datenübermittlung erläutert. Abschliessend erfolgt eine Gruppierung der Datenarten des grenzüberschreitenden Verkehrs und eine Uebersicht über die verschiedenen Arten internationaler Datenflüsse.

Zum rechtlichen Aspekt des grenzüberschreitenden Datenverkehrs bietet ein Ueberblick über die bestehenden Regelungen des grenzüberschreitenden Datenverkehrs in den verschiedenen nationalen Datenschutzgesetzen Europas (§ 9) einen analytischen Vergleich, aus dem de lege ferenda gewisse Schlussfolgerungen (hinten 3. Teil) für die nationale Ebene gezogen werden können. Im Anschluss an die nationalen Regelungen werden die von internationalen Gremien verabschiedeten Abkommen kritisch betrachtet (§ 10).

Im dritten Teil werden die aus den vorangehenden Ausführungen gewonnenen Erkenntnisse zu Lösungsvorschlägen ausgearbeitet.

Als Vorbereitung für die Lösungsvorschläge dient eine Differenzierung der Erscheinungsformen des grenzüberschreitenden Datenverkehrs, d.h. des Exportes, des Importes und des Transits, und die Konsequenz dieser Unterscheidung für eine rechtliche Regelung (§ 11). In § 12 werden die Probleme, die sich aus verschiedenen Datenschutzgesetzen bzw. deren Fehlen ergeben, für die nationale und internationale Ebene aufgezeigt. Im Hinblick auf einen möglichen Lösungsansatz wird eine Analyse der verschiedenen Anknüpfungspunkte und -prinzipien vorgenommen und die daraus resultierenden Folgerungen für ein internationales Abkommen bzw. dessen Mitgliedstaaten gezogen.

Nach diesen Schlussfolgerungen werden de lege ferenda Lösungsvorschläge für den nationalen Bereich ausgearbeitet. Sie beschränken sich nicht allein auf die Regelung des transnationalen Datenverkehrs, vielmehr wird versucht, diese Vorschläge in einem Gesamtkonzept eines nationalen Datenschutzgesetzes zu integrieren. Die Vorschläge zur

materiell- und formellrechtlichen Ausgestaltung des grenzüberschreitenden Datenverkehrs sind deshalb in allgemeinen Ausführungen zum Anwendungs-, Schutz und sachlichen Geltungsbereich sowie Massnahmen und Sanktionen eingebettet, die Voraussetzungen eines wirksamen Datenschutzes bilden. Im letzten Paragraphen (§ 14) werden Lösungsvorschläge für den internationalen Bereich dargelegt; sie gehen z.T. über die bestehenden internationalen Vereinbarungen und Abkommen hinaus, z.T. bauen sie auf diesen auf und zeigen als Lösungskonzept ein "internationales Rechtsregime i.S. einer Magna Charta des Datenschutzes".

I N H A L T S V E R Z E I C H N I S

<u>VORWORT</u>	I
<u>INHALTSUEBERSICHT</u>	III
<u>INHALTSVERZEICHNIS</u>	VII
<u>LITERATURVERZEICHNIS</u>	XXI
<u>PERIODICA</u>	XLV
<u>ABKUERZUNGSVERZEICHNIS</u>	XLVII
<u>EINLEITUNG</u>	LIII

I. TEIL: HAUPTASPEKTE IM PROBLEMKREIS DES GRENZUEBERSCHREITENDEN DATENVERKEHRS UND DESSEN REGELUNG ZUM SCHUTZE PERSONENBE- ZOGENER DATEN	1
--	---

<u>§ 1 NOTWENDIGKEIT DES GRENZUEBERSCHREITENDEN DATENVERKEHRS</u>	1
---	---

I. Ursachen des grenzüberschreitenden Datenverkehrs	1
1. Internationale Oeffnung	1
2. Wirtschaftliche und technische Gründe	2
3. Bedürfnis nach speziellen Informationsquellen	3
4. Sicherheitsgründe	3
5. Unternehmensbedingte Gründe	3
6. Andere Ursachen	3
II. Benutzer des grenzüberschreitenden Datenverkehrs	4
1. Tätigkeiten multinational operierender Gesellschaften	4
A. Multinationale Gesellschaften	4
B. Zwischengesellschaftlicher internationaler Datenverkehr	6
2. Datenaustausch zwischen nationalen Behörden und Regierungen	6
3. Datenaustausch multi und supranationaler Organisationen	7
III. Folgerung	8

<u>§ 2 PROBLEME DES PERSOENLICHKEITSSCHUTZES</u>	9
--	---

<u>§ 3 WIRTSCHAFTLICHE PROBLEME</u>	14
I. Beschäftigungsgrad	14
1. Positive Wirkung	14
2. Negative Wirkung	15
II. Zahlungsbilanzprobleme	15
III. Beeinflussung der einheimischen technologischen Entwicklung	16
 <u>§ 4 ABHAENGIGKEITSPROBLEME</u>	 17
I. Bedrohung der nationalen Sicherheit	17
II. Gefährdung der nationalen Souveränität	18
III. Gefährdung der nationalen Identität	20
IV. Der politische Aspekt: Dritte Welt und Entwicklungsländer	21
 <u>§ 5 DER GRENZUEBERSCHREITENDE DATENVERKEHR IM SPANNUNGSVERHAELTNIS ZWISCHEN FREIEM INFORMATIONSFLUSS UND SCHUTZ PERSONENBEZOGENER DATEN</u>	
I. Prinzip des freien Datenflusses	23
II. Einschränkungen des Datenflusses	24
1. Das legitime Interesse eines Staates	24
2. Die supranationalen Bestrebungen mehrerer Staaten	25
III. Persönlichkeitsschutz	25
1. National	25
2. International	27
A. Europäische Menschenrechtskonvention	27
B. Allgemeine Erklärung der Menschenrechte	27
C. Internationaler Pakt über bürgerliche und politische Rechte	27
D. Resolutionen des Europarates	28
IV. Informationsfreiheit	28
1. National	28
2. International	28
A. Europäische Menschenrechtskonvention	29
B. Internationaler Pakt über bürgerliche und politische Rechte	29
C. Konferenz über Sicherheit und Zusammenarbeit in Europa	30
D. Zwischenstaatliche Verträge	30
V. Bedeutung dieser internationalen Abkommen für den grenzüber- schreitenden Datenverkehr	30

<u>§ 6 DATA HAVENS</u>	33
I. Der Begriff	33
1. Datenoasen im nationalen Sinne	33
2. Datenoasen im grenzüberschreitenden Sinne	33
II. Gefahren beim grenzüberschreitenden Datenverkehr	34
III. Ursache von "data havens"	36
1. Nicht tarifliche Datenhindernisse	36
2. Tarifliche Datenhindernisse	36
IV. Technische Voraussetzungen für "data havens"	36
V. Auswahl eines "data havens"	37
VI. Vermeidung von "data havens"	37
1. Internationaler Fernmeldevertrag	39
2. INTELSAT-Abkommen	41
3. UNESCO Deklaration zur Satellitenübertragung	41
4. Internationales Rechtsvakuum	42
VII. Schlussfolgerung	44

II. TEIL: GRENZUEBERSCHREITENDER DATENVERKEHR	46
---	----

§ 7 BEGRIFF	46
-------------	----

I. Traditionelle Art der Uebermittlung	46
II. Automatisierte Uebermittlung	47

§ 8 ERSCHEINUNGSFORMEN DES GRENZUEBERSCHREITENDEN DATENVERKEHRS	49
---	----

I	Datennetze	49
1.	Begriffsbestimmung	49
2.	Arten von Netzen	49
	A. Oeffentliche Datennetze	49
	B. Gemeinschaftliche Datennetze	50
	C. Private Datennetze	51
3.	Entwicklungstrends	51
4.	Internationale Uebermittlungsmedien	53
II.	Träger von Datennetzen	55
1.	Im privaten Bereich	55
	A. SITA	55
	a) Träger	55
	b) Aufbau und Struktur des SITA-Netzes	56
	c) Klassierung der Daten	57
	d) Uebermittlungsobjekt	59
	aa) Reservationssysteme	59
	bb) Anwendungen der Flugabfertigung	60
	cc) Zusätzliche Applikationen	61
	dd) nichtflugreisespezifische Benutzungsarten	61
	e) Sicherung	61
	f) Geheimhaltung	61
	g) Verantwortlichkeit	62
	h) Folgerung	63
	B. SWIFT	64
	a) Träger	64
	b) Entstehungsgeschichte	64
	c) Aufbau und Struktur	64
	d) Zielsetzung	65
	e) Uebermittlungsobjekt	65
	f) Speicherung der Mitteilungen	67
	g) Sicherungsmassnahmen	67
	h) Schutz der sach- und personenbezogenen Angaben bei der Uebermittlung	68

i)	Verantwortlichkeit	69
k)	Zulässigkeitsvoraussetzungen für Mitgliedschaft beim SWIFT	70
l)	Statistische Angaben	71
m)	Folgerung	71
C.	Multinationale Gesellschaften: z.B. IBM	73
a)	Die Idee der Netzwerke, bzw. die Zielsetzung des "networking"	73
b)	Uebersicht der verschiedenen Netze	74
aa)	Innergesellschaftliche Netze	74
aaa)	Netze zur Verkaufsunterstützung und Geschäftsführung	74
11)	IBM E/ME/A Network (SWITCH)	75
22)	Corporate Consolidated Data Network	77
bbb)	Corporate Job Network (CJN)	79
11)	Ausdehnung	79
22)	Topologie	80
33)	Anwendungsbereich	80
bb)	Dienstleistungsnetz: European Personal Computing Service (EPCS)	81
aaa)	Struktur	81
bbb)	Zielsetzung	82
ccc)	Datensicherungsmassnahmen	83
ddd)	Natur der Daten	84
c)	RESPOND-Uithoorn International Network (SWITCH)	85
aa)	Internationale Applikationen	85
aaa)	HONE	85
11)	Aids	85
22)	Erif	86
33)	APL-Programmierung	87
44)	Script	87
55)	FTS	88
66)	Demo	88
77)	PROP	88
bbb)	ETS2	88
ccc)	FIS	92
ddd)	SECOM	92
eee)	RETAIN	93
fff)	IBTS	93
bb)	Beispiele der Benutzung von Anwendungsprogrammen	95
aaa)	Beispiel einer internationalen Applikation	95
bbb)	Beispiel einer nationalen Applikation	96
cc)	Datensicherung und Datenschutz	97
d)	Folgerung	99
2.	Im öffentlichen Bereich	101
A.	Euronet-Diane	101
a)	Aufbau und Träger	101
b)	Zielsetzung	103
c)	Charakteristika des Euronet-Diane	103

d)	Natur der Daten	104
e)	Datensicherung	104
f)	Folgerung	106
B.	O.I.P.C.-Interpol	109
a)	Anmerkung	109
b)	Allgemeines	109
c)	Zweck	110
d)	Struktur und Aufbau des Interpol-Netzes	110
e)	Natur der Daten	111
f)	Informationsfluss	112
aa)	Innerhalb der Organisation	112
bb)	Ausserhalb der Organisation	112
g)	Datenschutz	113
h)	Folgerung	115
III.	Andere Formen der Datenübermittlung	119
IV.	Arten von Daten, die den grenzüberschreitenden Verkehr bilden	121
1.	Klassierung	121
A.	Im privaten Bereich	121
a)	Daten der Produktions- und Vertriebskontrolle	121
b)	Daten der finanziellen Bewirtschaftung und Planung	122
c)	Daten über Arbeitnehmer und Gehaltsabrechnungen	123
d)	Daten finanzieller Transaktionen	123
e)	Reisereservationsdaten	123
f)	Daten der Marktbeobachtung und -analyse	124
B.	Im öffentlichen Sektor	124
a)	Daten von Regierungsstellen und öffentl. Behörden	124
b)	Daten der wissenschaftl. Forschung und Entwicklung	125
c)	Medizinische Daten	125
d)	Daten der Umweltüberwachung	125
2.	Umfang	126
3.	Konsequenz	126
V.	Arten der internationalen Datenflüsse	129
1.	Datenflüsse zwischen nationalen Gesellschaften und nationalen, rechtlich unselbstständigen Niederlassungen im Ausland	129
2.	Datenflüsse zwischen nationalen und ausländischen Gesellschaften	129
3.	Datenflüsse zwischen nationalen Gesellschaften und öffentlichen Stellen im Ausland	130
4.	Datenflüsse zwischen nationalen Behörden des öffentlichen Rechts und öffentlich-rechtlichen Stellen im Ausland	130
5.	Datenverarbeitung im Ausland im Auftrag eines nationalen Unternehmens oder einer öffentlichen nationalen Stelle	131
6.	Datenflüsse innerhalb von internationalen Organisationen	132

§ 9	<u>VERGLEICHENDER UEBERBLICK GESETZLICHER REGELUNGEN</u>	133
I	Umfang	133
1.	Allgemeine Grundzüge nationaler Gesetze	133
A.	Anwendungsbereich	133
B.	Bereich der geschützten Subjekte	136
C.	Sachlicher Geltungsbereich	137
2.	Rechtliche Regelung des grenzüberschreitenden Datenverkehrs in bestehenden Datenschutzgesetzen	137
II.	Vergleich bestehender Datenschutzgesetze	138
1.	Bundesrepublik Deutschland: Bundesdatenschutzgesetz	138
A.	Allgemeines	138
a)	Anwendungsbereich	138
b)	Schutzbereich	140
c)	Geltungsbereich	141
B.	Die rechtliche Regelung des grenzüberschreitenden Datenverkehrs	143
a)	Im öffentlichen Bereich: § 11 BDSG	145
b)	Im privaten Bereich: § 24 BDSG	146
C.	Folgerung	149
a)	Datenausfuhr	149
b)	Dateneinfuhr	155
2.	Oesterreich: Datenschutzgesetz	158
A.	Allgemeine Grundzüge des DSG	158
a)	Anwendungsbereich	158
b)	Schutzbereich	163
c)	Geltungsbereich	164
B.	Rechtliche Regelung des grenzüberschreitenden Datenverkehrs	166
a)	Datenexport	166
aa)	Allgemeines	166
bb)	Bestimmung des Begriffes "Uebermitteln"	168
cc)	Materielle Zulässigkeitsvoraussetzungen der Uebermittlung im öffentlichen Bereich	171
dd)	Materielle Zulässigkeitsvoraussetzungen der Uebermittlung im privaten Bereich	173
ee)	Formale Voraussetzungen für die Zulässigkeit von Uebermittlungen ins Ausland	174
aaa)	Grundsatz	174
bbb)	Ausnahme	176
ccc)	Weitere formelle Vorschriften	179
ff)	§ 34 Abs. 1 DSG	179
b)	Datenimport	180
aa)	Allgemeines	180
bb)	Materielle Voraussetzungen	181
cc)	Formelle Voraussetzungen	181
dd)	§ 34 Abs. 2 DSG	183
c)	Exkurs: Begriffsbestimmung des 'direkten Zugriffs'	183

C. Folgerung	185
3. Internationale Übersicht	189
A. Allgemeines	189
B. Gesetzesmodelle	189
a) Institutionelles Modell	189
b) Organisatorisches Modell	190
C. Schweden	191
a) Export personenbezogener Daten	191
b) Import personenbezogener Daten	195
D. Frankreich	196
a) Export personenbezogener Daten	197
aa) Für den privaten Bereich	197
bb) Für den öffentlichen Bereich	200
cc) Für beide Bereiche geltende Bestimmungen	200
b) Import personenbezogener Daten	202
E. Dänemark	203
a) Export personenbezogener Daten	203
aa) Gesetz über private Register	203
bb) Gesetz über öffentliche Register	206
b) Import personenbezogener Daten	207
c) Folgerung	207
F. Norwegen	209
a) Export personenbezogener Daten	209
b) Datenimport	210
c) Spezielle Norm für internationale Aktivitäten	210
d) Folgerung	234
G. Luxemburg	212
a) Export personenbezogener Daten	212
b) Import personenbezogener Daten	215
c) Folgerung	218
III. Typenbeschreibung der rechtlichen Regelungen des grenzüberschreitenden Datenverkehrs	220
1. Absolutes Exportverbot	222
2. Exportverbot mit Erlaubnisvorbehalt	224
A. Begriff	224
B. Abstufungen des Genehmigungssystems	224
a) Einzelgenehmigung	224
b) Mustergenehmigung	226
c) Konzession	228
3. Beschränkt freier Datenexport mit Verbotsvorbehalt	231
A. Systematische Einordnung	231
a) Einreihung unter das Exportverbot mit Erlaubnisvorbehalt	231
b) Einreihung unter den genehmigungsfreien Datenexport	231
c) rechtlicher Unterschied und Konsequenz	231
B. Inhalt des beschränkt freien Exportes	232
C. Voraussetzungen	233
D. Bedeutung	233

4. Genehmigungsfreier Datenexport	234
A. Begriff	234
B. Erscheinungsform	235
C. Folgerung	236
5. Schlussfolgerung	236

<u>6 10 BESTREBUNGEN INTERNATIONALER ORGANISATIONEN</u>	238
---	-----

I. Die Resolutionen des Europarates	239
II. EUROPARAT: Datenschutz-Konvention	242
1. Vorbemerkung	242
2. Inhalt der Konvention	242
A. Präambel und allgemeine Bestimmungen	242
a) Präambel	242
b) Zweck	243
c) Definitionen	244
d) Beschränkungs- und Ausdehnungsmöglichkeit des Anwendungsbereiches	249
aa) Beschränkung des Anwendungsbereiches	249
bb) Ausdehnung des Anwendungsbereiches	249
B. Bestimmung des materiellen Rechts in Form von Grundprinzipien	250
a) Ueberführung der Prinzipien ins nationale Recht	251
b) Grundprinzipien	251
aa) Qualität der Daten	251
bb) Spezielle Datenkategorien	252
cc) Datensicherung	253
dd) Zusätzliche Schutzmassnahmen	253
ee) Ausnahmen und Einschränkungen zum Datenschutz	255
gg) Ausdehnung des Schutzes	256
C. Spezielle Regeln zum grenzüberschreitenden Datenverkehr	257
D. Mechanismen für gegenseitige Rechtshilfe zwischen Signatarstaaten	261
a) Allgemeine Zusammenarbeit	261
b) Rechtshilfe für ausländische Datensubjekte	262
c) Spezifikation des Rechtshilfebegehrens	263
d) Schutzmassnahmen zur Rechtshilfe	263
e) Abweisung eines Rechtshilfebegehrens	264
f) Kosten und Verfahren der Rechtshilfe	265
g) Konsultativ-Komitee	266
E. Territorialklausel	266
3. Folgerung	267
III. OECD: Richtlinien zum Datenschutz	271
1. Vorbemerkung	271
2. Form der Richtlinien	271

3. Inhalt der Richtlinien	271
A. Teil I. und Präambel	272
a) Präambel	272
b) Teil I.	272
aa) Anwendungsbereich	272
bb) Ausnahmen	273
B. Teil II.	274
a) Ziel und Zweck	274
b) Inhalt der einzelnen Prinzipien	275
C. Teil III.: Prinzipien auf internationaler Ebene	277
D. Teil IV.	279
E. Teil V.	279
a) Internationale Zusammenarbeit	279
b) Gesetzes und Zuständigkeitskonflikte	281
F. Folgerung	281
IV. Europäisches Parlament: Empfehlungen an die EG-Kommission und den EG-Rat	282
V. Schlussfolgerung	283

III. TEIL: SCHLUSSFOLGERUNG UND LOESUNGSVORSCHLAEGE	284
---	-----

§ 11 DIFFERENZIERUNG DES GRENZUEBERSCHREITENDEN DATENVERKEHRS HIN- SICHTLICH EINER RECHTLICHEN REGELUNG	284
--	-----

I. Export	284
1. Ausfuhr von Daten aus inländischen Datensammlungen auf aus- ländische Verarbeitungsmedien oder Datensammlungen	286
2. Zugriff auf inländische Datenbanken mit personenbezogenen Informationen vom Ausland her	287
II. Import	289
1. Einfuhr von Daten ausländischer Datensammlungen auf in- ländische Datenverarbeitungssysteme	290
2. Zugriff auf ausländische Datenbanken vom Inland aus	291
III. Transit	293

§ 12 DAS SOG. "CONFLICT OF LAW"-PROBLEM BEIM GRENZUEBERSCHREITENDEN DATENVERKEHR. DIE SICH BEI VORLIEGEN VERSCHIEDENER DATENSCHUTZ- GESETZE BZW. BEI DEREN FEHLEN ERGEBENDEN PROBLEME	295
---	-----

I. Auf nationaler Ebene	295
1. Kollisionsprobleme	295
A. Ueberlappungen	296
B. Gesetzeslücken	296
C. Materiell widersprüchliche Gesetzesregelungen	297
2. Reaktion des Gesetzgebers	297
3. Notwendigkeit einer Kollisionsnorm ?	298
4. Die sich bei Vorliegen verschiedener Kollisionsnormen ergebenden Probleme	298
5. Schaffung einer Kollisionsnorm	299
II. Auf internationaler Ebene	300
1. Allgemeine Problematik des anwendbaren Rechts	300
2. Probleme und Lösungsmöglichkeiten der Bestimmung des an- wendbaren Rechts im Rahmen einer internationalen Konvention	302
A. Lösungsansätze und -möglichkeiten	302
a) Ausgangspunkt	302
b) Prinzip der Anknüpfung bzw. Frage der Zuständigkeit	304

c)	Mögliche Anknüpfungspunkte	306
aa)	Anknüpfung am Wohnsitz des Datensubjektes	306
aaa)	Vorteile	307
bbb)	Nachteile	308
ccc)	Folgerung	309
bb)	Anknüpfung am Ort der Verarbeitungshandlung, d.h. am Ort, wo der Verarbeitungsvorgang stattfindet	310
aaa)	Vorteile	310
bbb)	Nachteile	311
ccc)	Folgerung	312
cc)	Anknüpfung am Ort der Benutzungshandlung bzw. am Ort jedes Benützers der Daten	313
aaa)	Vorteile	314
bbb)	Nachteile	314
ccc)	Folgerung	315
dd)	Anknüpfung am Wohnort oder Geschäftssitz der verantwortlichen Stelle	316
aaa)	Vorteile	317
bbb)	Nachteile	318
B.	Schlussfolgerung	321
C.	Beschränkung des Anwendungsbereiches durch ein Kon- ventionsmitglied	322
3.	Kollisionsprobleme im Verhältnis von Konventionsstaaten zu Drittstaaten	322
A.	Begriff der Drittstaaten	322
B.	Problem	323
C.	Lösungsmodell	324
D.	Weitere Differenzierung der Drittstaaten	329
§ 13	LOESUNGSVORSCHLÄGE FÜR DEN NATIONALEN BEREICH, INSBESONDERE IM HINBLICK AUF EIN SCHWEIZERISCHES DATENSCHUTZRECHT	330
I.	Vorbemerkung	330
II.	Grundsätzliche Überlegungen zu den allgemeinen Aspekten eines Datenschutzgesetzes	331
1.	Ausgangspunkt	331
2.	Zielsetzung eines schweizerischen Datenschutzrechts	331
3.	Anwendungsbereich i.w.S.	333
A.	Anwendungsbereich i.e.S.	333
B.	Bereich der geschützten Subjekte (Schutzbereich)	337
a)	Schutz von Daten juristischer Personen	337
aa)	Argumente für eine Ausdehnung des Schutzes	337
bb)	Argumente gegen eine Ausdehnung des Schutzes	341
b)	Schutz von Daten, die Personengruppen und Rechts- gemeinschaften ohne Rechtspersönlichkeit betreffen	345
c)	Folgerung	346
C.	Sachlicher Geltungsbereich	348

III. Materiell und formellrechtliche Ausgestaltung des grenzüberschreitenden Datenverkehrs	351
1. Notwendigkeit einer speziellen Regelung des grenzüberschreitenden Datenverkehrs in einem nationalen Gesetz	351
2. Differenzierung der rechtlichen Ausgestaltung im privaten Sektor	351
A. Datenverkehr zwischen verschiedenen unabhängigen Stellen	352
B. Datenverkehr innerhalb von multinationalen Gesellschaften	352
C. Datenverkehr zwischen Stellen, die im Auftrag für Dritte Daten verarbeiten	354
3. Ausfuhr personenbezogener Daten	355
A. Voraussetzungen	355
a) Formelle	355
aa) Prinzip	355
bb) Zweck	356
b) Materielle	358
B. Grundsatz: Exportregelung ohne Berücksichtigung einer internationalen Vereinbarung.	358
a) Export von Ursprungsdaten	359
b) Wiederexport von importierten Daten	362
c) Zugriff auf inländische Datenbanken	362
C. Ausnahme: Exportregelung im Hinblick auf internationale völkerrechtliche Vereinbarungen (z.B. Konvention)	364
a) Fall des Exportes in Mitgliedstaaten der Konvention	364
b) Fall des Wiederexportes an Drittstaaten	365
4. Einfuhr personenbezogener Daten	366
A. Voraussetzungen	366
B. Grundsatz: Importregelung ohne Berücksichtigung einer internationalen Vereinbarung	366
a) Import von Daten ausländischen Ursprungs	366
b) Wiederimport exportierter Daten	367
c) Zugriff auf ausländische Datenbanken	367
C. Ausnahme: Importregelung im Hinblick auf internationale völkerrechtliche Vereinbarungen	368
a) Grundsatz: Garantie des freien Datenimportes aus dem Vertragsgebiet	368
b) Ausnahme: Genehmigung für Importe aus dem Konventionsgebiet	369
5. Transit	370
A. Sonderregelung für Transitdatenflüsse	370
B. Verletzung oder unbefugte Eingriffe in Transitdaten	372
C. Vorbehalt einer abweichenden Regelung durch ein internationales Rechtsregime	372
6. "Rechtshilfe" i.S. von Rechtsbeistand	372
A. Regelung ohne Berücksichtigung einer internationalen Vereinbarung	372
a) Legitimation	373

b)	Gegenstand der Rechtshilfe bzw. des Rechtsbeistandes	373
aa)	Wahrung der Individualrechte	374
aaa)	Individualrechte in nichtstreitigen Verfahren	374
bbb)	Individualrechte in streitigen Verfahren	374
bb)	Kostenlast	375
cc)	Unterstützung einer verantwortlichen Stelle	376
c)	Vollstreckung ausländischer Urteile und Entscheidungen	377
B.	Regelung im Hinblick auf eine internationale Vereinbarung	377
C.	Massnahmen zum Schutz der Rechtshilfe	377
7.	Bestimmung über die Datenqualität im internationalen Bereich	378
8.	Spezielle Datensicherungsvorkehrungen	379
III.	Massnahmen und Sanktionen bei Verletzungen materieller und formeller Normen zum grenzüberschreitenden Datenverkehr	380
1.	Zuordnung der Verantwortlichkeit	380
2.	Zweck und Inhalt	381
IV.	Verhältnis des grenzüberschreitenden Datenverkehrs zum Art. 273 StGB	383
V.	Nationale Kollisionsnormen	385
 <u>§ 14 LOESUNGSVORSCHLÄGE FÜR DEN INTERNATIONALEN BEREICH</u>		 390
I.	Lösungsmöglichkeiten zum Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr	390
1.	Harmonisierung nationaler Gesetze	390
2.	Vereinbarung minimaler Grundprinzipien	391
3.	Internationales Abkommen zur Regelung des grenzüberschreitenden Datenverkehrs	392
II.	Lösungskonzept: Internationales Rechtsregime zum Datenschutz	394
1.	Form	394
2.	Gründe und Argumente	395
A.	Für ein internationales Rechtsregime	395
B.	Gegen ein internationales Rechtsregime	398
3.	Konzeption	399
4.	Inhalt	400
A.	Zielsetzung	400
B.	Allgemeine Bestimmungen	401
C.	Grundprinzipien des Datenschutzes	402
D.	Bestimmungen zum grenzüberschreitenden Datenverkehr	404
E.	Kollisionsnormen	407
F.	Rechtshilfe und Zusammenarbeit der Behörden	409
G.	Spezialbestimmungen	411
III.	Schlussfolgerung	412

LITERATURVERZEICHNIS

- ANDREWS, Wright H.: An Overview of the emerging Statutory "Right" of Information Privacy, in: Law and computer technology, Vol. 10, No. 4, S. 82ff.
- AUERNHAMMER, Herbert: Auf dem Weg zu einem europäischen Datenschutzrecht, in: DS+DS, Heft 4, Oktober 1980, S. 181f.
- Bundesdatenschutzgesetz: Handkommentar, 1. Aufl., Köln, Berlin, Bonn, München 1977.
- Basic Issues in Data Protection Legislation and its International Harmonisation, in: OECD ICCP1, S. 298ff.
- AWV: Beiträge zum Bundesdatenschutzgesetz - BDSG, Teil 1, Eschborn, April 1977. (AWV = Ausschuss für wirtschaftliche Verwaltung in Wirtschaft und öffentlicher Hand e.V.).
- Beiträge zum Bundesdatenschutzgesetz - BDSG, Teil 2, Eschborn, August 1977.
- Beiträge zum Bundesdatenschutzgesetz - BDSG, Teil 3, Eschborn, September 1977.
- BAER, Rolf: Persönlichkeitsschutz der juristischen Person, in: ZBJV 103 (1967), S. 100ff.
- BARREIRO, J.: Le réseau de transmission de données espagnol, in: OECD ICCP1, S. 205ff.
- BASTIN, J.: Les flux de données transfrontières dans le domaine de l'assurance-crédit, in: OECD ICCP1, S. 127ff.
- BECKER, Ernst Eugen: Das dänische Datenschutzgesetz, in: OeVD 7-8/79, S. 3ff.
- BECKLER, D.: Closing Remarks, in: OECD ICCP1, S. 318ff.
- BEDNAR, Kurt;
WEISSENBOECK, Martin: Datenschutzhandbuch, Wien 1979.
- BENJAMIN, Alan A.: Privacy and Computers, in: OECD ICCP1, S. 174ff.
- Privacy, Security and Responsibility, in: Online - Transnational data regulation, S. 1ff.

- BERGMANN, Lutz;
MOEHRLE, Roland: Datenschutzrecht - Handkommentar zum Bundesdatenschutzgesetz, Stuttgart, München, Hannover 1977, (Ergänzungslieferung 1979).
- BERNASCONI, F.A. National Information Policies to Determine Transnational Data Regulation, in: Online - Transnational data regulation, S. 9ff.
- BERNHARD, U.;
GOLA, P.;
TUNER, L: Uebersetzung des französischen Datenschutzgesetzes, in: DS+DS, Heft 3, Juli 1978, S. 157f.
- BING, Jon: Norwegian Research Center for Computers and Law, in: Information Privacy, Vol. 1, No. 4, March 1979, S. 175ff.
- Norwegian Data Protection Legislation out of Deadlock, in: TDR, Vol. 2, No. 5, March 1979, S. 6/10.
- Transborder Data Flows - Some Legal Issues and Possible Effects on Business Practices, in: Online - Transnational data regulation, S. 15ff.
- BRANSCOMB, Lewis M.: Die letzten Grenzen der Information, in: NZZ, Nr. 241 vom 17.10.1979, S. 65f.
- BROUWER, G. E.: Transborder Data Flows and the Protection of Privacy: Australian Perspectives, in: OECD ICCP1, S. 267ff.
- BRUDERER, Herbert E.: Anschluss der Schweiz an Euronet-Diane (Eröffnung des Netzwerkknotens in Zürich), in: NZZ Nr. 252 vom 29. Okt. 1980, S. 36.
- Die Schweiz ist angeschlossen an Europas Datenstrom, in: sysdata + bürotechnik 11/79, S. 17f.
- Aufbauarbeit für "EURONET" in der Schlussphase - Anschluss der Schweiz für 1980 vorgehen, in: NZZ Nr. 134 vom 13. Juni 1978, S. 15.
- BUCHER, Eugen: Die Ausübung der Persönlichkeitsrechte, insbesondere die Persönlichkeitsrechte des Patienten als Schranken der ärztlichen Tätigkeit, Diss. Zürich, 1956.
- BULL, Hans Peter: Zur verfassungsrechtlichen Verankerung des Datenschutzes, in: OeVD 11/79, S. 3ff.

- BULL, Hans Peter: Datenschutz contra Amtshilfe (von der "Einheit der Staatsgewalt" zur "informationellen Gewaltenteilung"), in: Die öffentliche Verwaltung, Oktober 1979, 32. Jg., Heft 19, S. 689ff.
- Datenschutz als Informationsrecht und Gefahrenabwehr, in: NJW 23/1979 vom 6.6.79, 32. Jg., S. 1177ff.
- BUNDESBEAUFTRAGTER
FÜR DEN DATENSCHUTZ: Zweiter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäss §19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes, Deutscher Bundestag, 8. Wahlperiode, Drucksache 8/3570, Bonn, 1980.
- Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäss §19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG), dem Deutschen Bundestag vorgelegt zum 1. Januar 1979, Bonn 1979.
- BURKERT, Herbert;
ENGEL, Stefan: Datenschutz in Europa in: DS+DS, Heft 3, Juli 1980, S. 146ff.
- Die dänischen Datenschutzgesetze, in: DS+DS, Heft 1, Februar 1980, S. 43ff.
- BURKERT, Herbert;
ENGEL, Stefan;
JOHNSEN, Kjetil: Das norwegische Personendaten-Register-Gesetz, in: DS+DS, Heft 4, Oktober 1979, S. 252ff.
- BURNAND, Yves: Banques de données électroniques et droit de l'information, Diss. Lausanne 1974.
- BUTLER, R.E.: The International Telecommunication Union (ITU), in: OECD ICCP1, S. 197ff.
- CARMODY, Frank: Background to Data Protection in Europe, in: Information Privacy, Vol. 1, No. 1, September 1978, S. 24ff.
- The Role of the European Parliament in Data Protection, in: OECD ICCP1, S. 231ff.
- CARROLL, J.M.: The Problem of Transnational Data Flow, in: OECD Infomatics Studies, No. 10, S. 201ff.
- CASTLE, James: Network Information Services: The Essential International Business Tool, in: Online - Transnational data regulation, S. 29ff.

- CITTI, L.: Scientific and Technical Information and Data Transmission Networks: Impact at the National Level, in: OECD Summaries, S. 36.
- COMBS, William M.: Worldwide Data Communications a Reality, in: Online - Transnational data regulation, S. 189ff.
- CONRADI, Joachim: Empfehlungen des Euroäischen Parlamentes zur Harmonisierung des Datenschutzrechtes, in: DSWR 11/79, S. 247.
- CONSEIL DE L'EUROPE: Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, in: European Treaties Series / Série des traités européens, N° 108, Strasbourg 1981.
- Rapport explicatif concernant la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, in: Série des traités européens, N° 108, Strasbourg 1981.
- Comité Européen de Coopération juridique Rapport de Réunion, Addendum I., 33ème Réunion (septième réunion en tant que Comité Directeur), Strasbourg, 23-27 juin 1980; Strasbourg, 2 juillet; Restricted, CDCJ (80) 28.
- Projet de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, in: Rapport de Réunion, CDCJ (80) 28, Annexe III, S. 12ff.
- Les problèmes de conflits de loi d'autorités et de juridictions posés par le projet de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Rapport présenté par le Professeur Jean-Marie BISCHOFF, Strasbourg (Expert consultant). Restricted Document: CJ-PD (80) 2 Strasbourg, 8.4.1980.
- Protection de la vie privée des personnes vis-à-vis des banques de données électroniques dans le secteur public. Résolution (74) 29 adoptée par le Comité des Ministres du Conseil de l'Europe le 20 septembre 1974 et Rapport explicatif, Strasbourg 1975.

- COUNCIL OF EUROPE: The Council of Europe's Work In The Area Of Computers And Privacy - Discussion Paper - (Round Table on the use of data processing for Parliamentary Work), Strasbourg 18/19 May 1978.
- Final Statement (Round Table on the use of data processing for Parliamentary Work), Strasbourg 18/19 May 1978; AS/Science/RT (78)11.
- Information Bulletin of the Directorate of Legal Affairs of the Council of Europe, Legal Supplement No. 15 / February 1977, (v.a. S. 14).
- Protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. Resolution (73) 22 adopted by the Committee of Ministers of the Council of Europe on 26 september 1973 and Explanatory Report, Strasbourg 1974.
- European Conventions and Agreements, Vol. II., 1961-1970, Strasbourg 1972.
- CUNDIFF, W.E.: Issues in Canadian/US Transborder Computer Data Flow, in: Information Privacy, Vol. 1 No. 2, November 1978, S. 53ff.
- DAMMANN, Ulrich;
MALLMANN, Otto;
SIMITIS, Spiros: Die Gesetzgebung zum Datenschutz - Data Protection Legislation (Eine internationale Dokumentation - An International Documentation), Frankfurt 1977.
- DAMMANN, Ulrich;
SIMITIS, Spiros: Bundesdatenschutzgesetz (BDSG) mit Materialien, Baden-Baden 1977.
- DE CAPITANI, Werner: Ein Computergesetz ?, in: Bulletin 10/73, S. 7ff. (monatliche Zeitschrift der SKA).
- DEUTSCHER BUNDESTAG: Stenographisches Protokoll über die öffentliche Informationssitzung des Innenausschusses des Deutschen Bundestages vom 6. Mai 1974, 7. Wahlperiode - 724 - 2450 - Protokoll Nr. 37.
- DREWS, H. - L.: Synopse der den nicht öffentlichen Bereich betreffenden Novellierungsvorschläge zum BDSG, in: DS+DS, Heft 2, April 1980, S. 89f.

- DIEBOLD MANAGMENT
REPORT: Die Maschen der Netze, in: Diebold Management Report, Oktober/November 1977, S. 12ff.
- DREYFOUS, Etienne: International Trade and Transborder Data Flows, in: OECD ICCP1, S. 81.
- DUSCHANEK, Alfred: DSG - Datenschutzgesetz 1978: Für die Praxis erläutert, Wien 1978.
- EGER, John M.: Privacy Legislation in the USA, in: Information Privacy, Vol. 1, No. 6, July 1979, S. 244ff.
- US vs Miller and the right to financial privacy, in: Information Privacy, Vol. 1, No. 5, May 1979, S. 230f.
- Transnational Data Flow: the Need for Action, in: Computerworld, 13/2/1978, S. 15.
- Alliance for World Communications, in: Online - Transnational data regulation, S. 33ff.
- EGGER, August: Kommentar zum Schweizerischen Zivilgesetzbuch (Zürcher Kommentar), 1. Band: Einleitung und Personenrecht, Zürich 1930.
- EGLOFF, Willi: Braucht die Schweiz ein Datenschutzgesetz?, in: ZSR 96 (1977) Band 1, S. 345ff.
- EIDG. JUSTIZ- UND
POLIZEIDEPARTEMENT: Zivilrechtlicher Persönlichkeitsschutz, Zusammenstellung der Vernehmlassungen zu Vorentwurf und Schlussbericht der Expertenkommission für die Ueberprüfung des zivilrechtlichen Schutzes der Persönlichkeit (Revision der Artikel 28 ZGB und 49 OR) vom Dezember 1974, publiziert im April 1978.
- ELDIN, G.: Allocution, in: OECD ICCP1, S. 34ff.
- ENGELHARD, Helmut: Satellitendirektfernsehen - Neue Technologie für einen besonderen internationalen Informationsfluss ? Frankfurt, Bonn, Las Vegas 1978.
- ERICKSSON, Allan: The Vulnerability of Society, in: TDR, Vol. 1, No. 5, November 1978, S. 13f.

EUROPAEISCHE GEMEINSCHAFTEN (EG):

Beschluss des Rates vom 9. Oktober 1978 zur Festlegung eines zweiten Dreijahres Aktionsplanes im Bereich der wissenschaftlich-technischen Information und Dokumentation (78/887/EWG), in: Amtsblatt der Europäischen Gemeinschaften, Nr. L 311, S. 1ff. vom 4.11.1978.

EUROPAEISCHE MENSCHENRECHTSKONVENTION:

Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. Nov. 1950, in: AS 1974 II, S. 2151ff.

EUROPARAT:

Mitteilungen des Europarates, Beilagen für Rechtsfragen Nr. 10; Mitteilungsblatt der Rechtsabteilung des Europarates, Strasbourg, April 1974, (S. 8).

EUROPEAN PARLIAMENT:

Recommendations from Parliament to the Commission and Council Pursuant to Paragraph 10 of the Motion for a Resolution concerning: the principles which should form the basis of Community norms on the protection of the right of the individual in the face of developing technical progress in the field of data processing, in: TDR, Vol. 2, No. 2, May 1979, TDR Supplement, S. 7ff.

EXPERTENKOMMISSION
LUECHINGER:

Schlussbericht der Expertenkommission für die Überprüfung des zivilrechtlichen Schutzes der Persönlichkeit, Dezember 1974.

FABRY, Joseph:

Computerized Transfer of Legal Information between Nation, - Possibilities and Necessities, in: Law and computer technology, 3rd Quarter 1977, Volume 10, No. 3, S. 56ff.

FIERHELLER, G.A.:

A Canadian Viewpoint on the Problems of Transborder Data Flows, in: OECD ICCP1, S. 168ff.

FIRNBERG, David:

Security Standards for Transborder Data Flows, in: OECD ICCP1, S. 65ff.

FISHMAN, William L.:

International Data Flow: Some brief Thoughts on the View from The United States, in: Online - Transnational data regulation, S. 41ff.

FLEINER, Fritz;
GIACOMETTI, Zaccaria:

Schweizerisches Bundesstaatsrecht, Zürich 1976.

- FORSTMOSER, Peter: Grundfragen und Lösungsmöglichkeiten einer Datenschutzgesetzgebung, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 30ff.
- Ein schweizerisches Datenschutzgesetz?, in: NZZ Nr. 156, 8./9. Juli 1978, S. 31.
- Der Einsatz von Computern und das ärztliche Berufsgeheimnis, in: Schweizerische Ärztezeitung, Nr. 19, 8.5.1974, S. 729ff.
- FORSTMOSER, Peter;
MEIER-HAYOZ, Arthur: Einführung in das schweizerische Aktienrecht, 2. Aufl., Bern 1980.
- FRANK, Richard: Der Schutz der Persönlichkeit in der Zivilrechtsordnung der Schweiz, in: AcP 172 (1972) S. 56ff.
- FREESE, Jan: Data Policy in Sweden, in: Information Privacy, Vol. 1, No. 5, May 1979, S. 226ff.
- International Data Flow, Lund (S) 1979.
- Preserving the Open Flow of Information Across Borders, in: OECD ICCP1, S. 293ff.
- The Swedish Data Act, in: Online - Transnational data regulation, S. 187ff.
- GALLWAS, Hans-Ulrich;
SCHNEIDER, Jochen;
SCHWAPPACH, Jürgen;
SCHWEINICH, Joachim;
STEINBRINCK, Tilo: Datenschutzrecht. Kommentar und Vorschriften-sammlung, Stuttgart, Berlin, Köln, Mainz 1978.
- GARZON, Gregorio;
VILARINO, Eduardo: Information and Privacy Protection in Transborder Data Flows: The Rights Involved, in: OECD ICCP1, S. 302ff.
- GASSMANN, Hans-Peter: New International Policy Implications of the Rapid Growth of Transborder Data Flows, in: Online - Transnational data regulation, S. 209ff.
- Entwicklung des Datenschutzrechtes in Europa und Uebersee, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 59ff.

- GASSMANN, Hans-Peter: New International Policy Implications of the rapid Growth of Transborder Data Flows, in: OECD ICCPI, S. 51ff.
- GASSMANN, Hans-Peter;
PIPE, G. Russel: Synthesis Report, in: OECD Informatics Studies, No. 10, Paris 1976, S. 12ff.
- GERWIG, Andreas: Initiativen von Nationalrat Gerwig vom 22. März 1977, betreffend Persönlichkeits- und Datenschutzgesetz (Initiativen Gerwig v. 22.3.1977), abgedruckt in: SJZ 73 (1977), S. 244.
- GLORIES, J.: The s.i.t.a. story, Paris 1973.
- GOLDWATER Jr.,
Barry M.: Transnational Data - Facing Realities, in: Online - Transnational data regulation, S. 227ff.
- GOTLIEB, Allan;
DALFEN, Charles;
KATZ, Kenneth: The Transborder Transfer of Information By Communications And Computer Systems: Issues and Approaching to Guiding Principles, in: The American Journal of International Law, Vol. 68, 1974, S. 227ff.
- GROSSEN, J.-M.: Banques de données électroniques et protection de la personnalité - un aspect de la relation entre le progrès technique et la politique juridique, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 3ff.
- Das Recht der Einzelperson, in: Schweizerisches Privatrecht, Band 2, Basel 1967, S. 285ff.
- La protection de la personnalité en droit privée; quelques problèmes actuels, in: ZSR 70 (1960) Bd. II, S. 1a ff.
- GRUENHUT, Max: Schutz der Persönlichkeitssphäre im englischen und amerikanischen Recht, in: Zeitschrift für die gesamte Rechtswissenschaft, 74 (1962), S. 51ff (319ff).
- GULDENER, Max: Schweizerisches Zivilprozessrecht, 3. Auflage, Zürich 1979.

- GURADZE, Heinz: Die Europäische Menschenrechtskonvention - Konvention zum Schutze der Menschenrechte und Grundfreiheiten nebst Zusatzprotokollen, Berlin/Frankfurt 1968.
- HALLET, H. V. D.: Police and Transborder Data Flows, in: OECD ICCP1, S. 106ff.
- HAUSER, Marc Thomas: Informationsbeschaffung als Rechtsproblem, Diss. Zürich 1978.
- HAUSHEER, Heinz: Verstärkter Persönlichkeitsschutz: Der Kampf ums Recht an verschiedenen Fronten, in: Festgabe für Henri Deschenaux, Fribourg 1977.
- HEREDERO, M.: Avant-projet de loi espagnol sur les flux transfrontières de données, in: OECD ICCP1, S. 276ff.
- HERGENHAHN, Gerhard: Verbreitete Missverständnisse um das Bundesdatenschutzgesetz, in: DS+DS, Heft 1, Juli 1977, S. 25ff.
- HINDERLING, Hans: Persönlichkeit und subjektives Recht, Basler Studien zur Rechtswissenschaft, Heft 66, Basel 1963.
- HOLLEAUX, André: La loi du 6 Janvier 1978 sur l'informatique et les libertés, in: La revue administrative, 31e année, 1978, No. 181/182, S. 32ff/160ff.
- HONDIUS, Frits: Data Legislation on the march, in: Information Privacy, Vol. 1, No. 1, September 1978, S. 4ff.
- The Action of the Council of Europe with Regard to International Data Protection, in: OECD ICCP1, S. 257ff.
- The Council of Europe's Data Protection Principles, in: Online - Transnational data regulation, S. 47ff.
- International Data Protection Action, in: OECD Informatics Studies 10, S. 208ff.
- HOTZ, Kaspar: Zum Problem der Abgrenzung des Persönlichkeitsschutzes nach Art. 28 ZGB, Diss. Zürich, 1967.
- HUBMANN, Heinrich: Das Persönlichkeitsrecht, Köln-Graz 1967.
- HUG-BEELI, Gustav: Wo liegt die Grenze der persönlichen Freiheit?, Diss. Zürich, 1976.

- HUMMEL, E.: The Role of CCITT in Data Communication (CCITT = Comité consultatif International Télégraphique et Téléphonique), in: OECD ICCP1, S. 202ff.
- IBM: Fortschritte in der Computer Spracherkennung, in: NZZ, Nr. 1980, 6. Aug. 1980, S. 37.
- Fachausdrücke der Text- und Datenverarbeitung, Wörterbuch und Glossar: Englisch-Deutsch / Deutsch-Englisch, Stuttgart 1978.
- INTERPOL: International Criminal Police Organization: Constitution and General Regulations, Paris 1968 (mit Nachträgen).
- JAEGGI, Peter: Fragen des privatrechtlichen Schutzes der Persönlichkeit, in: ZSR 79 (1960), Band 2, S. 133a ff.
- JOHNSON, Timothy: Data Networks and International Data Traffic in Europe, in: Online - Transnational data regulation, S. 155ff.
- JOINET, Louis: Le projet de la loi français relatif à l'informatique et aux libertés, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 68ff.
- Les aspects juridiques, économiques et sociaux des flux transfrontières de données personnelles, in: OECD ICCP1, S. 208ff.
- JUCKER, Ulrich: Neue Leistungen der Fernmeldedienste der PTT - Rapider Vormarsch der Teleinformatik, in: NZZ Nr. 134 vom 11. Mai 1979, S. 35f.
- KAMLAH, Ruprecht: Right of Privacy, Köln 1969.
- KASPERS, Elmar: Die Einordnung des Datenschutzbeauftragten in multinationalen Konzernen, in: DS+DS, Heft 2, April 1980, S. 82ff.
- KELLER, Max;
SIEHR, Kurt: Einführung in die Eigenart des Internationalen Privatrechts, 2. Aufl., Zürich 1979.
- KENNY, Joe: UK Data Protection Committee Report: A Discussion, in: Information Privacy, Vol. 1, No. 4, March 1979, S. 183ff.
- KEPLINGER, M.: Information and Documentation Services, in: OECD ICCP1, S. 153ff.

- KIAR, Palle: Competition and Cooperation: the Canadian Experience in National and Trans-national Data Communications, in: Online - Transnational data regulation, S. 171ff.
- KIMMICH, Gerhard;
SIMON, Klaus: Daten über Satellit, in: IBM Nachrichten (IBM Deutschland) Nr. 249 April 1980, 30. Jg., S. 47ff.
- KIRBY, M. D.: Developing International Rules To Protect Privacy, in: Law and computer technology, 3rd Quarter 1979, Volume 12, No. 3, S. 53ff.
- KRONEBERG, D.: Telecommunications for Air Transportation, in: OECD ICCP1, S. 183ff.
- KSZE: Phraseologie der KSZE Schlussakte, Hrsg. Auswärtiges Amt der BRD, Bonn 1977.
- KUMMER, Max: Der zivilrechtliche Schutz des Persönlichkeitsrechtes, in: ZBJV 103 (1967), S. 106ff.
- LAICHER, E.: Der Datei-Begriff in der Praxis, in: DS+DS, Heft 3, Juli 1978, S. 61.
- LANNOY, J.: Les communautés européennes et l'information scientifique et technique, in: OECD ICCP1, S. 147ff.
- LARESE, Wolfgang: Persönlichkeitsschutz und Massenmedien, Anmerkungen zur Revision von Art. 28 ZGB, in: NZZ Nr. 149, 30.6./1.7. 1979, S. 37.
- LARSSON, Torsten: The Nordic Public Data Network, in: OECD ICCP1, S. 188ff.
- The Introduction of Public Data Networks as an Example of Expanding Telecommunication Services, in: Online - Transnational data regulation, S. 55ff.
- LAUTSCH, John: Law and Computer Privacy in the States of the USA, in: Information Privacy, Vol. 1, No. 3, January 1979, S. 100ff.
- LAYTON, Christopher: Protection of Privacy - Future Prospects at the European Communities Level, in: OECD ICCP1, S. 213ff.
- LEHMANN, Beat: Datenschutz bei grenzüberschreitendem Datenverkehr: Die OECD-Richtlinien vom 23. September 1980, in: sysdata + bürotechnik, 12/1980, S. 10f.

- LEHMANN, Beat: Datenschutz bei grenzüberschreitendem Datenverkehr: Die Konvention des Europarates vom 17. September 1980, in: sysdata + bürotechnik, 11/1980, S. 10f.
- Neue Datenschutzgesetze: Luxemburg, in: sysdata + bürotechnik, 7/1979, S. 11.
- LEMOINE, Philippe: International Information Trade, in: TDR, Vol. 2, No. 1, March 1979, S. 12.
- LINDEMANN, P.: Datenschutzrecht (BDSG) und Persönlichkeitsrecht, in: DS+DS, Heft 4, Oktober 1979, S. 221ff.
- LINDOP, Norman: International Protection of Personal Data - Reciprocity or Harmonisation?, in: OECD ICCP1, S. 288ff.
- LIVER, Peter: Der gesetzliche Schutz der Persönlichkeit in der Rechtsentwicklung, in: ZBJV 103 (1967) S. 80ff.
- LONGSWORTH, M. A.: Transborder Data Flows and the Protection of Privacy, in: OECD ICCP1, S. 74ff.
- MAAS, Hans Heinrich: Information und Geheimnis im Zivilrecht, Münchner Universitätsschriften, Band 4, Stuttgart 1970.
- MALLMANN, Otto: The Transborder Movement and Protection of Data - Relevant International Agreements and Organisations, OECD, Paris 25th July 1977, DSTI/ICCP/77.18.
- Zielfunktionen des Datenschutzes; Schutz der Privatsphäre - korrekte Information. Mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen, Frankfurt a/M. 1977.
- MARTIN-LØF, J.: Introductory Remarks, in: OECD ICCP1, S. 39ff.
- MAX-PLANCK-INSTITUT: Der zivilrechtliche Persönlichkeits- und Ehrenschatz in Frankreich, der Schweiz, England und den Vereinigten Staaten von Amerika, Gutachten, Tübingen 1960.
- MEIER-HAYOZ, Arthur;
FORSTMOSER, Peter: Grundrisse des schweizerischen Gesellschaftsrechts, 3. Aufl., Bern 1978.

- MEISTER, Herbert: Aspekte einer Novellierung des Bundesdatenschutzgesetzes, in: DS+DS, Heft 3, Juli 1980, S. 123ff.
- Transborder Data Flows - Ein Thema für die Internationale Handelskammer, in: DS+DS, Heft 2, April 1980, S. 72ff.
- Europäische Harmonisierung des Datenschutzes, in: DS+DS, Heft 1, Februar 1980, S. 9ff.
- MICHEL, J.: L'impact des réseaux de transmission de données, in: OECD ICCP1, S. 144ff.
- MORAN, P.: Transborder Data Flows Associated with Computer Systems in Australian Government Departments, in: OECD ICCP1, S. 97.
- MUELLER, Jörg Paul: Die Grundrechte der Verfassung und der Persönlichkeitsschutz des Privatrechts, Bern 1964.
- MUTTER, Peter: Persönlichkeitsschutz und Datensicherung - Überlegungen zur Durchführbarkeit und zu den Kosten, Computer und Recht, Bd. 9, Zürich 1980.
- NAGEL, Kurt: Datenschutz und Datensicherung: Begriffe, Bestimmungsfaktoren, Realisierung, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 10ff.
- NORMANN, Adrian R. D.: Project GOLDFISH, in: Online - Transnational data regulation, S. 67ff.
- A Scheme for Regulating Transborder Data Flows, in: TDR, Vol. 1, No. 7, December 1978, S. 18ff.
- Project Goldfish (Global Online Data Files and Information System Haven), in: Information Privacy, Vol. 1, No. 1, September 1978, S. 8ff.
- NOWAK, R.: Data Protection in Transborder Data Flows in the Banking Sector, in: OECD ICCP1, S. 124ff.
- OCDE: Utilisation des Réseaux Internationaux de Transmission des Données en Europe; Politiques d'Information d'Informatique et de Communication (PIIC2), Paris 1979.

- O'CONNOR, D.: Public Administration (Taxation and Social Insurance), in: OECD ICCP1, S. 92ff.
- OECD: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Adopted by the Council at its 523rd Meeting on 23rd September, 1980), Paris 1st October, 1980, in: Dok. Nr.: C (80) 58 (Final).
- Explanatory Memorandum: Appendix to the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, in: Recommendation, Dok. Nr.: C (80) 58 (Final), S. 9ff.
- Transborder Data Flows and the Protection of Privacy, Proceedings of a Symposium held in Vienna, Austria; 20th-23rd September 1977, Information Computer Communications Policy (ICCP1), Paris 1979.
- Background Document for Participants (Vienna Symposium), in: OECD ICCP1, S. 14ff.
- Summaries of papers; Symposium on Transborder Data Flow and Protection of Privacy, - Trends and Impacts - Vienna 20th-23rd September 1977; Paris, 26th August 1977; DSTI/ICCP/77.36.
- Policy Issues in Data Protection and Privacy - Concepts and Perspectives - Proceedings of the OECD Seminar 24th to 26th June 1974; OECD Informatics Studies, Vol. 10, Paris 1976.
- OFTINGER, Karl: Schweizerisches Haftpflichtrecht, Band 1, 4. Aufl., Zürich 1975.
- ONLINE Transnational data regulation, relevant notes from lectures presented at the conference - Transnational Data Regulation - Brussels, February 1978; England 1978.
- ONSTAD, P. C.: Data Processing Services and Transborder Data Flows, in: OECD ICCP1, S. 178ff.
- ORDEMANN, Hans-Joachim: Grenzüberschreitender Datentransport - Internationales Datenschutzübereinkommen, in: OeVD 6/77, S. 3ff.
- ORDEMANN, Hans-Joachim;
SCHOMERUS, Rudolf: Bundesdatenschutzgesetz, München 1977.

- OSBORN, Jack L.: Corporate Employee Information Handling Practices and Employee Perceptions, in: OECD ICCP1, S. 261ff.
- OSVALD, Thomas: Australian Privacy Legislation, in: Information Privacy, Vol. 1, No. 2, November 1978, S. 88f.
- PAHR, W.: Opening Address, in: OECD ICCP1, S. 31ff.
- PANTAGES, A.
PIPE, G.R.: A New Headache for International DP, in: Datamation Nr. 6, 1977, S. 118ff.
- PARSONS, C.: The U.S. Privacy Protection Study Commission, in: OECD ICCP1, S. 242ff.
- PAULSEN, J.: Rules for Transnational Data Flows, in: OECD Informatics Studies 10, S. 219ff.
- PAWLIKOWSKY, Gerhart J.: (Hrg.) Datenschutz - Leitfaden und Materialien, Wien 1979.
- Auf dem Weg zur Informationsgesellschaft, in: PAWLIKOWSKY: Datenschutz - Leitfaden und Materialien, S. 46ff.
 - Datenschutz im Betrieb, in: PAWLIKOWSKY: Datenschutz - Leitfaden und Materialien, S. 74ff.
 - Was bringt das österreichische Datenschutzgesetz?, in: DS+DS, Heft 1, Januar 1979, S. 22ff.
 - Datenschutz geht alle an;
 - Teil I in: IBM Oesterreich: Informationen, Berichte, Modelle; Heft November 1978.
 - Teil II in: IBM Oesterreich: Informationen, Berichte, Modelle; Heft Mai 1979.
 - Datensicherheit, Ergebnisse aus empirischen Studien zu Datenschutz und Datensicherheit, in: Data Press Wien, Heft 1 (1977), S. 7-11.
- PIERA, F.: Activities of the IBI (Intergovernmental Bureau for Informatics) in the Field of Transnational Data Flows, in: OECD ICCP1, S. 236f.
- PIPE, G. Russel: Transnational Data Regulation: Reviewing the Issues, in: Online - Transnational data regulation, S. 233ff.

- PIPE, G. Russel: French Study Urges Independence from US, in: Computerworld, 5. Sept. 1977, S. 5.
- PODLECH, Adalbert: Datenschutz im Bereich der öffentlichen Verwaltung, in: DVR, Beiheft 1, Berlin 1973.
- RAUCH, W.: Datensicherung in der Datenfernübertragung durch Verschlüsselung, in: DS+DS, Heft 4, Oktober 1979, S. 242ff.
- RAUSCH, Heribert: Das Persönlichkeitsrecht und der Schutz des Einzelnen vor verletzenden Pressebildern, Bern 1969.
- READ, Charles N.: Banking and the Regulation of Data Flows, in: OECD ICCP1, S. 139ff.
- REISINGER, Leo: BDSG und DSG - ein Vergleich der deutschen und österreichischen Datenschutzgesetzgebung, in: DS+DS, Heft 2, April 1979, S. 120ff.
- Das Begriffsfeld "Datenschutz", in PAWLKOWSKY: Datenschutz - Leitfaden und Materialien, S. 6ff.
- RETZLAFF, Werner: TYMNET - ein "kompatibles" Datenübertragungsnetz, in: OeVD, online/adl 11/79, S. 913f.
- RICHARDSON, J.M.: Some Observations about Barriers and Ease of Transborder Data Flow, in: OECD ICCP1, S. 310f.
- RODOTA, S.: Legislation et la libre circulation de l'information, in: OECD ICCP1, S. 308f.
- SAMET, P.A.: Transborder Dataflow, in: Information Privacy, Vol. 1, No. 5, May 1979, S. 231f.
- SARK
(SARBARHETSKOMMITTEN): The Vulnerability of the Computerized Society (preliminary report by a Swedish Government Committee), Stockholm 1978.
- SARTORIUS, Carl: Internationale Verträge - Europarecht, Band II, 14. Aufl., Stand 1.3.1979, München 1979.
- SCHEDL, Ilse: Bundesdatenschutzgesetz, 1. Aufl., Kissing 1977.
- SCHINDEL, Jost: Das französische Datenschutzgesetz vom 6.1.1978 - eine bürgerfreundliche Regelung, in: DSWR 10/1978, S. 232ff.

- SCHLANITZ, E.: Les flux de données transfrontières dans le contexte de la coopération policière internationale, in: OECD ICCP1, S.102ff.
- SCHNEIDER, J.: Datenschutz - Datensicherung, Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung, Band 5, Hg. Siemens AG, München 1971.
- SCHOMERUS, Rudolf: Grenzüberschreitender Datenverkehr (Unselbstständige Zweigstelle im Ausland - Dritter ?), in: DS+DS, Heft 1, Februar 1980, S. 7f.
- Grundzüge des Bundesdatenschutzgesetzes, in: Computer und Privatsphäre, Computer und Recht Band 6, Zürich 1978, S. 76ff.
- Das französische Datenschutzgesetz, in: DS+DS, Heft 2, April 1978, S. 61.
- Regulation of Trans-Frontier Data Traffic under the Federal Data Protection Law, in: Online - Transnational data regulation, S. 221ff.
- SCHUCAN, Jürg: Datenbanken und Persönlichkeitsschutz, Computer und Recht, Band 4, Zürich 1977.
- SCHULTZ, Hans: Einführung in den allgemeinen Teil des Strafrechts; Band 1 (Die allgemeinen Voraussetzungen der kriminalrechtlichen Sanktionen), 2. Auflage, Bern 1974.
- Zivilrechtlicher Schutz der Persönlichkeit und Strafrecht, in: ZBJV 103 (1967), S. 93ff.
- SCHWAPPACH, Jürgen: Internationale Datenflüsse im Bereich der Industrie und ihre Bewertung nach dem BDSG, in: DS+DS, Heft 1, Januar 1978, S. 21ff.
- Bundesdatenschutzgesetz (BDSG) mit Erläuterungen, Bergisch-Gladbach 1977.
- International Data Flows in the Industrial Sector, in: OECD ICCP1, S. 217ff.
- SCHWEIZER, Rainer J.: Der Stand der Datenschutzgesetzgebung in der Schweiz, in: DS+DS, Heft 3, Juli 1980, S. 153ff.
- Probleme und Realisierungsmöglichkeiten Datenschutzrechtes auf Bundesebene, in: Computer und Privatsphäre, Computer und Recht, Band 6, Zürich 1978, S. 112ff.

- SEIDEL, Ulrich: Telekommunikation und Datenschutz, in: DS+DS, Heft 1, Februar 1980, S. 40ff.
- SELIGMAN, N.: The Importance of Empirical Research, in: OECD-ICCP1, S. 86ff.
- SELMER, Knut: Norwegian Privacy Legislation, in: Information Privacy, Vol. 1, No. 4, March 1979, S. 178ff.
- SENDLER, Hans: Zur Subsidiarität des Bundesdatenschutzgesetzes, in: DS+DS, Heft 2, April 1979, S. 120ff.
- SERWATYNSKI, William: Transborder Dataflow: A global View, in: Information Privacy, Vol. 1, No. 3, January 1979, S. 133ff.
- Transborder Data Flow: Lifeblood of Multinationals, in: Information Privacy, Vol. 1, No. 2, November 1978, S. 81ff.
- SHIRAI, F.: Computer Communication in Japan, in: OECD ICCP1, S. 195ff.
- SIEGHART, P.: The Protection of Personal Data - Lacuna and Overlap, in: OECD ICCP1, S. 224ff.
- SIMITIS, Spiros: Grenzüberschreitender Datenaustausch - Notwendige Vorbemerkungen zu einer dringend erforderlichen Regelung, in: Konflikt und Ordnung, Festschrift für Murad Ferid, München 1978, S. 356ff.
- Ueber die Schwierigkeiten einer Datenschutzregelung - Zum Stand der Diskussion, in: SAG 47 (1975) Nr. 1, S. 1ff.
- Chancen und Gefahren der elektronischen Datenverarbeitung, in: Neue Juristische Wochenschrift 24 (1971), S. 673ff.
- SIMITIS, Spiros;
DAMMANN, Ulrich;
MALLMANN, Otto;
REH, Hans-J.: Kommentar zum Bundesdatenschutzgesetz, Baden-Baden 1978.
- SITA: Statistical Information, Type A + B Traffic, 2nd Quarter 1979, SI/T - 79018, 14. November 1979.

- SITA: Statistical Information, Type A + B Traffic, 1st Quarter 1979 SI/T - 79017, 19. Juli 1979.
- Articles of Association, Paris 1977.
- SITA - Was ist das?, Informationsbroschüre der S.I.T.A. - Niederlassung Zürich.
- SMITH, Robert Ellis: Compilation of State and Federal Laws on Privacy, published by Privacy Journal, Washington D.C. 1976.
- SPIEKER, W.: Data Protection and the Trade Unions, in: OECD ICCP1, S. 233ff.
- STADLER, Gerhard: Die Durchführungsverordnungen zum österreichischen Datenschutzgesetz, in: DS+DS, Heft 2, April 1980, S. 91ff.
- Erste Verwaltungserfahrungen mit dem österreichischen Datenschutzgesetz, in: Verwaltungspraxis 11-12/79, S. 11ff.
- Der Informationsverkehr zwischen Oesterreich und der Bundesrepublik Deutschland nach den Datenschutzgesetzen, in: Wirtschaftsbrief der Deutschen Handelskammer in Oesterreich 1979/11-12.
- Das neue Datenschutzgesetz von Luxemburg, in: OeVD 10/79, S. 8ff.
- Das Datenschutzgesetz und seine Auswirkungen in der Versicherungswirtschaft, in: Die Versicherungsgrundschau, Zeitschrift der österreichischen Gesellschaft für Versicherungsfachwissen, 34. Jg., Nr. 7/8, Juli/August 1979, S. 241ff.
- Eine künftige Datenschutzkonvention des Europarates und das bundesdeutsche und das österreichische Datenschutzrecht, in: DS+DS, Heft 3, Juli 1979, S. 169ff.
- Das österreichische Datenschutzgesetz - Die Zulässigkeit von Ermittlung, Verarbeitung und Uebermittlung personenbezogener Daten nach dem Datenschutzgesetz, IBM Oesterreich, Januar 1979 (IBM Form GAUS-0100).
- Wirtschaftsinformationen und Datenschutz, in: Oesterreichische Zeitschrift für Wirtschaftsrecht 1979, Nr. 1 (OeZW 1979/1), S. 9.

- STADLER, Gerhard: Internationaler Datenschutz 1978, in: OeVD 1-2/1979, S. 3f.
- Das österreichische Datenschutzrecht, in: PAWLIKOWSKY: Datenschutz - Leitfaden und Materialien, S. 46ff.
 - Das österreichische Datenschutzgesetz, in: OeVD 11/1978, S. 8ff.
 - Das französische Datenschutzgesetz vom 6. Januar 1978, in: OeVD 4/78, S. 22f.
 - To International Regulations on Data Flows and Privacy Protection, in: Online - Transnational data regulation, S. 95ff.
 - Grenzüberschreitender Datenverkehr und Datenschutz, in: OeVD, Online-adl-Nachrichten, 11/77, S. 923f.
 - Datenschutz zwischen Persönlichkeitsschutz und Informationsfreiheit, in: NZZ Nr. 266 vom 12./13. Nov. 1977 S. 37.
 - From National to International Legislation on Information Flow and Data Protection, in: OECD ICCP1, S. 42ff.
 - Erfahrungen mit dem Schwedischen Datengesetz, in: DSWR 4/1976, S. 99ff.
- STADLER-RICHTER, Helga: Möglichkeit der Weitergabe personenbezogener Daten von Studenten in Oesterreich, in: OeVD 6/79, S. 15.
- STARCK, Emil W.: Die Produkthaftungspflicht und die Tendenzen zu ihrer Vereinheitlichung in Europa, in: ZBJV, Bd. 114 (1978), S. 345ff.
- STEINMUELLER, Wilhelm: Computernetze und Informationsrecht, in: DVR, Bd. 8, Heft 3, 1979, S. 213ff.
- Fragestellungen der internationalen Datenschutzdiskussion, in: Datenschutz; Referate und Diskussion der Tagung "Datenschutz" der österreichischen Juristen-Kommission in Wien am 18./19. April 1975 (Dokumente zum Datenschutz, Hrsg.: Gerhard STADLER, Wien 1975).
 - Allgemeine Grundsätze zur rechtlichen Regelung des Datenschutzes, in: SCHNEIDER, Datenschutz - Datensicherung, S. 13ff.

- STEINMUELLER, Wilhelm: Vortrag zum Thema Datenschutz, gehalten im Rahmen des Seminars Computer und Recht an der Universität Zürich am 30.5.1975.
- STRATENWERTH, Günter: Schweizerisches Strafrecht, Besonderer Teil Band II.; Straftaten gegen Gemeininteressen, 2. Aufl., Bern 1978.
- STROEMBERG, G.: International Message Transfer between Banks, in: OECD ICCP1, S. 133ff.
- STRUEBY, Rolf: Datensicherheit - Die Verantwortung der Computerhersteller, in: Computer und Recht, Bd. 6, Zürich 1978, S. 126ff.
- SUERBOECK, Erich K.: Datenschutzpraxis in Oesterreich (organisatorische Massnahmen im privaten Bereich zum 1. Jänner 1980 einschliesslich Datenverarbeitungsregisterverordnung), Hrg. Arbeitsgemeinschaft für Datenverarbeitung (ADV), Wien 1980.
- SUTCLIFFE, Alan: Anatomy of Privacy and Data Protection, in: Information Privacy, Vol. 1, No. 6, July 1979, S. 255ff.
- SWIFT: SWIFT. Brochure about SWIFT, Brüssel 1979.
- TAIB, A.: Flux de données transfrontières - aspects culturels et économiques, in: OECD ICCP1, S. 293ff.
- TREILLE, Jean-Michel: L'information économique et industrielle: ses sources et ses canaux de distribution, in: OECD ICCP1, S. 160ff.
- TUBIES, H.: Amtshilfe und Datenschutz, in: DS+DS, Heft 2, April 1979, S. 75ff.
- TUETSCH, Hans E.: Schutz der Privatsphäre in Amerika - Gesetzesvorlagen gegen Missbräuche der Technik, in: NZZ Nr. 108 vom 6. April 1979, S. 7.
- TUOR, Peter;
SCHNYDER, Bernhard: Das Schweizerische Zivilgesetzbuch, 9. Aufl., Zürich 1975.
- TURN, Rein: Implementation of Privacy and Security Requirements in Trans-national Data Processing Systems, in: Online - Transnational data regulation, S. 113ff.
- UNESCO/IBI: Strategies and Policies for Informatics (SPIN-Conference, Malaga 1978), UNESCO Doc. SC/MD/63 vom 30.3.1979

- UNESCO: L'UNESCO et la protection des libertés individuelles, in: OECD ICCP1, S. 238ff.
- UTSUMI, Takeshi: International Marketing Mechanism of Computer Information Services, in: Online - Transnational data regulation, S. 133ff.
- VANDENBERGHE, Hugo: La vie privée et les banques de données, in: OECD ICCP1, S. 249ff.
- VESELSKY, E.: Concluding Statement, in: OECD ICCP1, S. 314ff.
- VINGE; P.G.;
(FREESE, Jan): Experiences of the Swedish Data Act, Stockholm, 1975.
- VISCHER, Frank: Internationales Privatrecht; 2. Nachdruck aus "Schweizerisches Privatrecht", Band I. (1969), Hrsg. M. Gutzwiler, H. Hinderling, A. Meier-Hayoz, H. Merz, R. Secrétan, W. von Steiger; Basel, Stuttgart 1973.
- VOSS, Heinz-Rudolf: SCHUFA und Bundesdatenschutzgesetz, in: DS+DS, Heft 3, Juli 1979, S. 183ff.
- WALCKIERS, P.: L'informatisation des controls douaniers - application aux flux des marchandises Europe-Moyen-Orient, in: OECD ICCP1, S. 111.
- WALDER, Hans-Ulrich: Der neue Zürcher Zivilprozess - ein Handbuch, 2. Aufl., Zürich 1979.
- WALLER, Richard: Code of Practice for Privacy, in: Information Privacy, Vol. 1 No. 1, September 1978, S. 22f.
- WALKER, Philip M.: Barriers to achieving the full potential of international data communications, in: Online - Transnational data regulation, S. 181ff.
- WALTERSKIRCHEN VON, Martin: Ausdehnung von "Euronet" auf die Schweiz, in: Europa (Hrg. Europa-Union Schweiz) vom 25. Juni 1979, S. 16f.
- WEISE, Karl-Theodor: Textverarbeitung und Datenschutz, in: DS+DS, Heft 3, Juli 1980, S. 139ff.
- WERMDALEN, Hans: International Data Transmission From the Users Point of View, in: OECD ICCP1, S. 69ff.
- WESTIN, Alan F.: Transborder Flows of Personal Health Data: A Problem Whose Time has not yet come, in: OECD ICCP1, S. 114ff.

- WESTIN, Alan F.: Der Mensch und seine Privatsphäre. Gedanken zum Freiheitsbegriff im technischen Zeitalter;
1. Teil: IBM Nachrichten 20 (1970) Nr. 201, S. 189ff.
2. Teil: IBM Nachrichten 20 (1970) Nr. 202, S. 289ff.
- WHITE, Robert B.: Conditions for Regulating Transborder Data Flows, in: TDR, Vol. 1, No. 7, December 1978, S. 17.
- WITTEK, H.: Grenzüberschreitender Datenverkehr (Unselbstständige Zweigstelle im Ausland - Dritter ?), in: DS+DS, Heft 2, April 1980, S. 69ff.
- WITTKAEMPFER, G.W.: Datenoasen - ein Mythologem ?, in: DS+DS, Heft 2, April 1978, S. 59f.

PERIODICA

Datenschutz und Datensicherung, (Braunschweig/Wiesbaden)	DS+DS
Datenverarbeitung im Recht (Berlin)	DVR
Datenverarbeitung in Steuer, Wirtschaft und Recht (München)	DSWR
Information Privacy (Haywards Heath, [Sussex]; New York)	
IBM Bulletin der IBM Schweiz (Zürich)	
IBM Nachrichten der IBM Deutschland (Stuttgart)	
Karlsruher juristische Bibliographie (München/Frankfurt)	KJB
Law and Computer Technology (Hrsg. World Peace Through Law Center, Washington D.C.)	
Monatsschrift für Deutsches Recht (München, Frankfurt)	MDR
Neue Juristische Wochenschrift (München Frankfurt)	NJW
Neue Zürcher Zeitung (Zürich)	NZZ
Oeffentliche Verwaltung und Datenverarbeitung OeVD/online/adl (Köln)	OeVD
Schweizerische Aktiengesellschaft (Zürich)	SAG
Schweizerische Juristenzeitung (Zürich)	SJZ
Transnational Data Report (Washington, D.C., Amsterdam)	TDR
Zeitschrift für Rechtspolitik (München, Frankfurt)	ZRP

ABKUERZUNGSVERZEICHNIS

a.a.0	am angeführten Ort
Abs.	Absatz
Add.	Addendum
ADV	Automatische Datenverarbeitung
A/FE	IBM World Trade Americas/Far East Corporation
AG	Aktiengesellschaft
AHV	Schweizerische Alters- und Hinterlassenen Versicherung
a.M.	anderer Meinung
Anm.	Anmerkung
Art.	Artikel
AS	Ämtliche Sammlung der Bundesgesetze und Verordnungen: Sammlung der Eidgenössischen Gesetze
AT&T	American Telephon and Telegraph Corp.
AufI.	Auflage
AWV	Ausschuss für wirtschaftliche Verwaltung in Wirtschaft und öffentlicher Hand e.V., (Eschborn [BRD])
B	Belgien
BB1.	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BDSG	Bundesdatenschutzgesetz: Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Daten- verarbeitung vom 27. Januar 1977
bes.	besonders
BF	Belgische Francs
BG	Bundesgesetz
BGB	Bürgerliches Gesetzbuch für das Deutsche Reich vom 18. Aug. 1896
BGB1.	Bundesgesetzblatt (Oesterreich, BRD)
BGE	Entscheidungen des Schweizerischen Bundesgerichts. Ämtliche Sammlung
BGr.	Bundesgericht
BKA	Bundeskriminalamt (BRD)
BRD	Bundesrepublik Deutschland
Bsp.	Beispiel
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1874
bzw.	beziehungsweise
ca.	zirka
CBEMA	Computer and Business Equipment Manufacturers Association
CCITT	Comité Consultatif International Télégraphique et Télé- phonique
CDC	Control Data Corporation
CDN	Kanada
CDU	Christlich demokratische Union (Deutschland)
cf.	confer, conférez = vergleiche
CH	Schweiz
CJN	Corporate Job Network
CNIL	Commission Nationale de l' Informatique et des Libertés (Frankreich)

Co.	Colorado (US-Bundesstaat)
Corp.	Corporation
CSU	Christlich soziale Union (Deutschland)
d.B.f.D	des Bundesbeauftragten für den Datenschutz
D.C.	District of Columbia
ders.	derselbe (Autor)
DES	Data Encryption Standard
d.h.	das heisst
DIANE	Direct Information Access Network for Europe
DIB	Data Inspection Board, (=Datainspektionen), Schweden
Diss.	Dissertation
DK	Dänemark
Doc.	Document
Dok.	Dokument
DP	Data Processing
DS+DS	Datenschutz und Datensicherung (Braunschweig/Wiesbaden)
DSG	Datenschutzgesetz (Oesterreich): Bundesgesetz über den Schutz personenbezogener Daten vom 18. Oktober 1978
DSWR	Datenverarbeitung in Steuer, Wirtschaft und Recht (München)
DTN	Data Transport System
DV	Datenverarbeitung
DVR	Datenverarbeitung im Recht (Berlin)
E	Spanien
E.	Erwägung
ECs	European Communications Satellite
EDS	Elektronisches Datenwählsystem
EDV	elektronische Datenverarbeitung
EEC	European Economic Communities (vgl. EG od. EWG)
EG	Europäische Gemeinschaften (vgl. EEC od. EWG)
E/ME/A	IBM World Trade Europe/Middle East/Africa Corporation
EMRK	Europäische Menschenrechtskonvention
EPCS	European Personal Computing Service
Erw.	Erwägung
ESA	European Space Agency
etc.	et cetera
e.V.	eingetragener Verein
ev.	eventuell
evtl.	eventuell
EWG	Europäische Wirtschaftsgemeinschaft (vgl. EEC od. EG)
f	und folgende (Seite, Note usw.)
F	Frankreich
FAO	Food and Agriculture Organisation (= Welternährungsorganisation)
FDP	Freie demokratische Partei (Deutschland)
ff	und folgende (Seiten, Noten, usw.)
Ga.	Georgia (US-Bundesstaat)
GB	Great Britain
GG	Grundgesetz der Bundesrepublik Deutschland
gl.A.	gleicher Ansicht
gl.M.	gleicher Meinung
GmbH	Gesellschaft mit beschränkter Haftung
h.M.	herrschende Meinung

Hrg.	Herausgeber
Hrsg.	Herausgeber
HW	Hardware
I	Italien
i.a.	im allgemeinen
IBI	International Bureau for Informatics
IBM	International Business Machines Corporation
ICCP	Information Computer Communications Policy (vgl. Literaturverzeichnis: OECD)
id.	idem = derselbe
i.d.R.	in der Regel
i.e.	id est = z.B.
i.e.S.	im engern Sinne
Ill.	Illinois (US-Bundesstaat)
int.	international
Intelsat	International Telecommunications Satellite Organization
intern.	international
IPR	Internationales Privatrecht
IRC	International Record Carriers
i.S.	im Sinne
i.S.v.	im Sinne von
ITU	International Telecommunications Union
i.V.	in Verbindung
IV	Schweizerische Invalidenversicherung
i.w.S.	im weitern Sinne
IZPR	Internationales Zivilprozessrecht
Jg.	Jahrgang
KE	Konvention des Europarates vom 17. September 1980
KIS	Kriminalpolizeiliches Informationssystem (Schweiz)
KSZE	Konferenz für Sicherheit und Zusammenarbeit in Europa
LDSG	Landesdatenschutzgesetz (Bundesländer der Bundesrepublik Deutschland)
LIFL	La loi No. 78-17 du 6.1.78 relative à l' informatique, aux fichiers et aux libertés
lit.	litera = Buchstabe
Ltd.	Limited
LUX	Luxemburg
m.a.W.	mit andern Worten
Md.	Maryland (US-Bundesstaat)
MDR	Monatsschrift für Deutsches Recht
m.E.	meines Erachtens
N	Note
NATO	North Atlantic Treaty Organization
NBS	National Bureau of Standards (US Department of Commerce)
NCS	Network Control System
NICS	NATO Integrated Communications System
NJW	Neue Juristische Wochenschrift (München/Frankfurt a.M.)
NL	Niederlande, Holland
No.	Numéro/Number
Nr.	Nummer
NR	Nationalrat
N.Y.	New York

NZZ	Neue Zürcher Zeitung
OCDE	Organisation de Coopération et de Développement économiques (vgl. OECD)
OECD	Organisation for Economic Co-operation and Development (vgl. OCDE)
OeVD	Oeffentliche Verwaltung und Datenverarbeitung (Köln)
OeZW	Oesterreichische Zeitschrift für Wirtschaftsrecht
O.I.P.C.	Organisation internationale de Police Criminelle
OR	BG über das Obligationenrecht vom 30. März 1911/ 18. Dez. 1936
OTS	Orbital Test Satellite
Pa.	Pennsylvania (US-Bundesstaat)
p.a.	per annum, pro Jahr
PIIC	Politiques d'Informations d' Informatique et de Communication (vgl. Literaturverzeichnis: OCDE)
PIN	Personal Identification Number
PTT	Post, Telegraph- und Telephon
Q.	Quartal
Res.	Resolution
resp.	respektive
RL	OECD-Richtlinien vom 23. September 1980
S.	Seite
SAG	Schweizerische Aktiengesellschaft (Zürich)
Sect.	Section
Sek.	Sekunde
Sinef	SITA Negative File
SITA	Société Internationale pour la Télécommunication Aéronautique
SJZ	Schweizerische Juristenzeitung
sog.	sogenannte
SPD	Sozialdemokratische Partei Deutschlands
SPIN	Strategies and Polisieis for Informatics
StGB	Schweizerisches Strafgesetzbuch vom 21. Dez. 1937
SW	Software
SWIFT	Society for Worldwide Interbank Financial Telecommunication s.c.
TDR	Transnational Data Report (Washington D.C./ Amsterdam
u.a.	und andere
u.ä.	und ähnliches
u.a.m.	und anderes mehr
U.K.	United Kingdom (England)
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNO	United Nations Organization
US	United States
USA	United States of America
usf.	und so fort
usw.	und so weiter
u.U.	unter Umständen
v.a.	vor allem
VE	Vorentwurf
vgl.	vergleiche
Vol.	Volume

WHO	World Health Organization = Weltgesundheitsorganisation
WMO	World Meteorological Organisation
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins (Bern)
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dez. 1907
ZH	Zürich
Ziff.	Ziffer
zit.	zitiert
ZPR	Zeitschrift für Rechtspolitik
ZSR	Zeitschrift für Schweizerisches Recht (Basel)
z.T.	zum Teil

EINLEITUNG

Die durch die Computertechnologie unterstützte Datenverarbeitung¹ hat sich von der anfänglich isolierten, stapelweisen Verarbeitung einzelner Arbeitsgebiete in knapp drei Jahrzehnten zur weltumspannenden Informationsverarbeitung² entwickelt. Durch die Kombination der Telekommunikationseinrichtungen mit der EDV wurden auch die Verarbeitungsorte physisch mobil.

Die erste Reaktion auf die Entwicklungen im Bereich der modernen Datenverarbeitungstechnologien resultierte in einer Gesetzgebungswelle während der 70er Jahre, in der auf einzelstaatlicher Ebene Anstrengungen unternommen wurden, die durch die automatische Datenverarbeitung bedrohte Privatsphäre zu schützen. Die Bemühungen und Arbeiten endeten in einer Normsetzung, die dem Individuum helfen, den Ueberblick über die ihn betreffenden Daten und deren Verarbeitung zu erhalten bzw. wiederzuerlangen, damit der Einzelne bei einer Persönlichkeitsverletzung die Möglichkeit hat, die aus dem Persönlichkeitsrecht fließenden Ansprüche einzuklagen.

Gleichzeitig eröffnete die technologische Entwicklung durch die Datenfernverarbeitung neue Perspektiven beim Erschliessen geographisch entfernter Verarbeitungsplätze. Damit war die Möglichkeit geschaffen, die Datenverarbeitung von rechtlich-normierten Territorien in Gebiete ohne Datenschutzvorschriften oder weniger restriktiven Bestimmungen zu verlagern. Die nationalen Gesetzgeber vermochten diesen neuartigen Aspekten deterritorialisierter Verarbeitungsvorgänge nur eine partielle Aufmerksamkeit zu verleihen, da es vorerst

-
- 1 Anfänglich diente der Computer und die Geräte der mittleren Datentechnik der reinen Kalkulationsverarbeitung.
 - 2 Nach einer gewissen Zeit nutzte man den Computer auch für direkte Bedürfnisse (Luftraumüberwachung, Flugreservation, Steuerungssysteme) und begann mit der Datenverarbeitung; basierend auf dieser Technologie wurden neue Bereiche erschlossen wie Textverarbeitung, electronic mail, Faksimile Uebertragung, Mikrofilmspeicherung und graphische Verarbeitung; die Zukunft wird auch die Sprach- und Bildverarbeitung mittels Digitaltechnik eröffnen und den Kreis der Informationsverarbeitung abrunden.

internen Regelung der Datenverarbeitungsvorgänge zum Schutz der Persönlichkeit bedurfte.

Ende der 70er Jahre führten die Erkenntnisse auf nationaler Ebene, bedingt durch das immer grösser werdende Ausmass der internationalen Datenverarbeitungsaktivitäten, zu einer zweiten Reaktion, die sich durch ihre internationale Dimension charakterisiert.

Für die 80er Jahre gilt es nun, den Schutz der Persönlichkeit von der nationalen Stufe auf die internationale Ebene auszudehnen und dabei die durch verschiedene Sprachen, Kulturen, Sitten und Rechtssysteme begründeten Schranken, Einzelinteressen, die ihre Ausprägung teilweise bereits in nationalen Gesetzen gefunden haben, abzubauen. Es bedarf überdies einer internationalen Normierung für eine koordinierte zwischenstaatliche Zusammenarbeit, Schutzmassnahmen und Sicherungsvorkehrungen, damit die Furcht vor wirtschaftlicher, technischer und politischer Abhängigkeit, durch missbräuchliche Verwendung der Ware Information, verringert werden kann und protektionistische Attitüden verschwinden.

Für Länder, die sich in der Gesetzgebungsphase oder im Novellierungsstadium des Datenschutzrechts befinden, gilt es, anhand der existierenden Arbeiten internationaler Gremien wie Europarat, die Informationspolitik der datenschutzbewussten Nationen zu erkennen und die nationalen Gesetzgebungsarbeiten darauf auszurichten, dass eine Integration des nationalen Gesetzes hinsichtlich der internationalen Dimension mit keinen Hindernissen verbunden ist, und dem Persönlichkeitsrecht bei den weltumspannenden Verarbeitungsvorgängen ein global gleichwertiger Schutz zuteil wird, der letztlich dem Einzelnen ermöglicht, die Kontrolle über die Zirkulation der ihn betreffenden Information auszuüben: Eine Macht, die die Grundlage der persönlichen Freiheit darstellt.

I. TEIL: HAUPTASPEKTE IM PROBLEMKREIS DES GRENZUEBERSCHREITENDEN DATENVERKEHRS UND DESSEN REGELUNG ZUM SCHUTZE PERSONENBEZOGENER DATEN

§ 1 NOTWENDIGKEIT DES GRENZUEBERSCHREITENDEN DATENVERKEHRS

Import und Export von Daten ist nicht neu und war immer schon möglich,¹ aber die Entwicklung der elektronischen Datenverarbeitung hat sich vom anfänglichen Schwerpunkt der Stapelverarbeitung über verschiedene Zwischenstufen (batch, online) weg auf die Datenfernverarbeitung verlagert und die Ein- und Ausfuhr von Informationen in grossem Umfang erst möglich gemacht; ein immer dichter werdendes Verbindungsnetz von Telephonleitungen - und seit neuester Zeit sogar von Satellitenübertragungen² - ermöglichen heute schon problemlos die interkontinentale Informationsbeschaffung und -verbreitung.

I. Ursachen des grenzüberschreitenden Datenverkehrs

1. Internationale Oeffnung

Die internationale Oeffnung der letzten Jahrzehnte, bedingt durch neue Technologien und Transportmedien, sowie die Intensivierung des internationalen Handels- und Wirtschaftsverkehrs hat zu einem

1 Z.B. auf manuelle Art: per Brief, Boten; auf automatische Art: per Telex, Telephon, Telegraph etc.

2 Am 7. Dez. 1980 wurde von Cape Canaveral der erste der Fernmeldesatelliten der Intelsat-5-Serie gestartet und in eine geostationäre Umlaufbahn über dem Atlantik gebracht; ab März 1981 soll der Betrieb aufgenommen werden. Er kann gleichzeitig zwei Fernsehprogramme und bis zu 12'000 Telefongespräche übertragen. Bis 1983 sollen insgesamt sieben bis neun Satelliten dieser Serie im Weltraum platziert werden: Je zwei über dem Atlantik, Indischen Ozean und Pazifik, wovon einer Stellvertreterfunktion hat. Die restlichen Satelliten werden nach Bedarf an andern Stellen positioniert.

Ziel ist, allen 105 der Intelsat angeschlossenen Mitgliedsländern ein lückenloses Uebertragungsnetz zu ermöglichen. Da alle Mitgliedstaaten über Bodenstationen für das Senden und den Empfang von Daten verfügen, darunter auch die Schweiz, wird ein weltumspannendes Datenübertragungssystem geschaffen. (Vgl. NZZ, Nr. 286 vom 8. Dez. 1980, S. 5).

verstärkten internationalen Informationsaustausch geführt. Gleichzeitig ist auch ein verstärktes Bedürfnis nach direkter zwischenstaatlicher Zusammenarbeit auf Behördenebene zu registrieren und, wo es um regionale³ bzw. kontinentale oder globale⁴ wirtschaftliche, kulturelle und politische Interessen geht, haben sich multi- und supranationale Organisationen gebildet. Diese international ausgedehnte Tätigkeit bedarf aber zur Erfüllung der angestrebten Ziele eines transnationalen Informationsverkehrs.

Letztlich erfordert die zunehmende Mobilität des Menschen über die nationalen Grenzen hinaus einerseits mehr Export und Import von Informationen,^{5 6} andererseits bietet der Datenaustausch dem Einzelnen Vorteile und Erleichterungen⁷ - teilweise werden solche bereits als Dienstleistungen erwartet.

2. Wirtschaftliche und technische Gründe

- Wirtschaftliche Ueberlegungen können ergeben, dass die routinemässige Verarbeitung von Daten aus Lohn- und Kostengründen oder geographischen Bedingungen⁸ im Ausland billiger ist.
- Bei speziellen Anforderungen einer Branche kann es vorkommen, dass ausländische Rechenzentren über technische Experten, Software und Lösungen verfügen, die lokal nicht zu bekommen sind.

3 Z.B. EG.

4 Z.B. UNO, UNESCO, INTERPOL.

5 Z.B. das Abkommen zwischen Kanada und der Bundesrepublik über Informationsaustausch von Sozialversicherung und andern Sozialleistungen.

6 HONDIUS sagt treffend: "when people are moving, their data move with them"(OECD Informatics Studies 10, S. 214).

7 Bekanntestes Beispiel sind die Sitzreservationen im Flugverkehr: am Abflugdatum erhält der Fluggast seinen reservierten Sitz ohne grosse Probleme (als angenehme Nebenerscheinung der Vorausbuchung können Flüge nach gewissen Destinationen erheblich billiger werden).

8 Es ist naheliegender, Daten von Vancouver (Kanada) nach Seattle (USA) zu senden, als nach Toronto (Kanada); ebenso kann es für ein im Vorarlberg tätiges Unternehmen günstiger sein, die Daten im Fürstentum Lichtenstein oder in der Schweiz verarbeiten zu lassen, als in Wien. Häufig ist eine Ansiedlung von DV-Betrieben in Grenzregionen zu beobachten (vgl. auch FREESE, Data Flow, S. 25f.).

- Auch die Ausnützung freier Verarbeitungskapazitäten während Nachtzeiten kann eine Verlagerung in ein Land mit anderer Zeitzone rechtfertigen.
- Die Benützung zentraler Dokumentations- und Informationssysteme erlaubt einen kostengünstigeren Unterhalt.

3. Bedürfnis nach speziellen Informationsquellen

Dieses Bedürfnis kann Anstoss zum grenzüberschreitenden Datenverkehr sein, wenn bestimmte aktuelle Informationen nur auf fremden, ausländischen Datenbanken verfügbar sind.⁹

4. Sicherheitsgründe

Aus Gründen der Datensicherheit kann es angebracht sein, Daten nicht nur im Inland, sondern auch im Ausland zu speichern oder ein (zweites) Datenverarbeitungssystem im Ausland zu benutzen, falls politische Verschiebungen oder Katastrophen, Sabotageakte oder ein schwacher Datenschutz im Inland ein Ausweichen auf das ausländische Datenverarbeitungssystem erfordern.¹⁰

5. Unternehmensbedingte Gründe

Die Tätigkeit multinationaler Gesellschaften setzt für deren Steuerung und Entscheidungen sowie zur Erfüllung gesetzlicher Vorschriften einen grenzüberschreitenden Datenverkehr voraus: z.B. zur Konsolidierung der Geschäftsdaten und Gewinnberechnung (zwecks Steuererhebung oder Dividendenausschüttungen), aber auch zur Kundenbetreuung, die ebenfalls in mehreren Ländern operieren, oder zur Personalpolitik.

6. Andere Ursachen

Auch die Existenz von Datenschutzgesetzen oder das bevorstehende Inkrafttreten eines solchen kann zur Verlagerung gewisser Datenbe-

9 Z.B. Telenet, Tymnet (USA) oder Euronet sowie andere technisch-wissenschaftliche Datenbanken.

10 Z.B. SWIFT: DV-Zentren in Holland und Belgien.

stände, deren Verarbeitung im betreffenden Territorium vom Gesetz nicht mehr oder nur unter gewissen Voraussetzungen erlaubt ist, in Länder ¹¹ führen, die keine einschränkenden Vorschriften kennen. Dieser Grund ist aber nicht als Primärursache für den grenzüberschreitenden Datenverkehr zu qualifizieren, sondern stellt einen Folgegrund dar.

Charakteristisch ist, dass die Daten meist in die Richtung des wirtschaftlichen Vorteils fließen.¹²

II. Benutzer des grenzüberschreitenden Datenverkehrs

1. Tätigkeiten multinational operierender Gesellschaften

Multinationale Gesellschaften und Verflechtungen von inländischen mit ausländischen Unternehmen ¹³ haben einen immer grösser werdenden Informationsbedarf verschiedenster Natur, der nicht mehr nur durch nationale Quellen gestillt werden kann, sondern internationale Verbindungen erfordert. Den volumenmässig grössten Anteil haben dabei Handels- und Industriegesellschaften.

A. Multinationale Gesellschaften

Die dominierenden Benutzer und Anwender des grenzüberschreitenden Datenverkehrs sind die multinationalen Gesellschaften.¹⁴ Es handelt sich hier fast ausschliesslich um einen innergesellschaftlichen Informationsfluss ¹⁵ auf firmeneigenen Datennetzen, um - den Austausch von internen administrativen und personellen Gesellschaftsinformationen abzuwickeln;

11 Vgl. hinten, S. 33ff., v.a. S. 37ff.

12 "Data havens", vgl. CAROLL, S. 203.

13 Z.B. Joint Ventures.

14 FREESE, Data Flow, S. 29.

15 Die meisten grossen Kreditkartengesellschaften, wie Master Charge, American Express, Visa, Diners Club etc., haben in den USA ihren Hauptsitz und ihre Rechenzentren: die im Ausland (Kanada, Zentralamerika) gemachten Ausgaben ihrer Klienten überqueren zur Nachführung der Kundenkonti die Grenzen und werden in den Rechenzentren der USA konsolidiert; (CARROLL, S. 201f., mit weiteren Beispielen).

- Antworten auf Kundenanfragen bezüglich gewisser Dienstleistungen mit möglichst grosser internationaler Unterstützung beantworten zu können;
- Kunden und andere Personen bzw. Unternehmen betreffende Angaben und Berichte zu erstellen und zu verwalten;
- von einer schnellen, zuverlässigen und kostengünstigen allgemeinen Informationsübermittlung und -beschaffung¹⁶ zu profitieren.

In beschränktem Umfang pflegen die multinationalen Unternehmen auch einen aussergesellschaftlichen internationalen Datenfluss; i.d.R. erfolgt die Informationsbeschaffung dieser Firmen durch die im betreffenden Lande tätige Zweigniederlassung bzw. Tochtergesellschaft, die normalerweise den Kontakt zu andern nationalen Unternehmen (z.B. Zulieferfirmen) unterhält, so dass der aussergesellschaftliche Informationsverkehr auf nationaler Stufe vollzogen wird.

Ein neues Betätigungsfeld multinationaler Gesellschaften ist das Anbieten von internationalen Datennetzen über Rechenzentren,¹⁷ die kleineren nationalen Unternehmen mit internationalem Tätigkeitsgebiet den kostspieligen Aufbau eines firmeneigenen Datennetzes ersparen¹⁸ und damit einer Vielzahl von Gesellschaften den grenzüberschreitenden Datenaustausch erst ermöglichen.

16 Electronic mail und firmeneigene Informationsdatenbanken.

17 Vgl. den European Personal Computing Service (EPCS) der IBM-Rechenzentren, (hinten, S. 81ff.). Dieser Service verbindet die wichtigsten europäischen Servicezentren in Belgien, Bundesrepublik, Dänemark, Finnland, Frankreich, Grossbritannien, Holland, Italien, Norwegen, Schweden, Schweiz, Spanien über einen in Holland stationierten Grossrechner untereinander. Die Datensicherheit wird durch eine Vielzahl von Sicherungsmassnahmen gewährleistet.

18 Die den einzelnen Kunden anfallenden Kosten sind begrenzt, - verglichen mit denen eines eigenen Datennetzes - da sie nur die Telefonkosten bis ins nächste Rechenzentrum des eigenen Landes (z.B. Zürich für die Schweiz) zu tragen haben, während bei internationalen Verbindungen bedeutend höhere Tarife anfallen. Zu den Gebühren müssen noch die normalen Datenverarbeitungskosten des Rechenzentrums veranschlagt werden.

B. Zwischengesellschaftlicher internationaler Datenverkehr

Neben den multinationalen Gesellschaften existiert aber auch ein beträchtliches Volumen an transnationalen Datenverschiebungen zwischen verschiedenen, voneinander unabhängigen Unternehmen. Viele dieser Firmen benützen dabei Datennetze: entweder fremde, d.h. von lokalen international tätigen Rechenzentren¹⁹ angebotene Dienste, die zur Verarbeitung ins Ausland übermittelt werden,²⁰ oder zu speziellen Zwecken geschaffene Datennetze,²¹ die von einer Interessengemeinschaft verschiedener nationaler Unternehmen der gleichen Wirtschaftsbranche²² getragen werden. Auf diesen Datennetzen wird ein aussergesellschaftlicher Informationsfluss mit sach- und personenbezogenen Angaben unterhalten.

Ausser dem Transfer über Datennetze existiert aber auch ein direkter Austausch von Informationen zwischen Gesellschaften verschiedener Länder, sei es durch point-to-point-connections oder durch konventionellen Transfer roher (d.h. nicht automatisiert verarbeiteter Daten) oder maschinenlesbarer Informationen.²³

2. Datenaustausch zwischen nationalen Behörden und Regierungen

Im Rahmen der in den letzten Jahren stark angestiegenen Zusammenarbeit in administrativen Belangen von öffentlich-rechtlichen Stellen²⁴ und Institutionen²⁵ verschiedener Länder ist der internationale Datenverkehr eine allgemein anerkannte Notwendigkeit geworden.^{26 27} Charakteristisch für den internationalen Datenaustausch

19 Z.B. CDC-Datennetz.

20 Oft wissen die Gesellschaften nicht einmal, wo die Daten, die dem Rechenzentrum anvertraut wurden, verarbeitet werden.

21 Z.B. SITA, SWIFT; vgl. hinten, S. 55ff. und 64ff.

22 Z.B. Banken und Kreditinstitute.

23 FREESE, Data Flow, S. 20; vgl. ferner hinten, § 7 S. 47.

24 Amerikanische und kanadische Steuerbehörden tauschen Einkommensdaten ihrer Landsleute aus, die jeweils im andern Lande Wohnsitz haben (CARROLL, S. 202f., mit weiteren Beispielen).

25 Z.B. verteilt Interpol im Rahmen der weltweiten Verbrechensbekämpfung Informationen über international tätige Verbrecher an ihre Mitgliedstaaten.

26 Z.B. auf dem Gebiet der Wettervorhersage, des Gesundheits- und Krankenwesens, etc.

auf öffentlich-rechtlicher Ebene ist die strikte Trennung zwischen den einzelnen nationalen Datenverarbeitungssystemen; die Verarbeitung von Daten durch Behörden verschiedener Staaten auf einem gemeinsamen System ist aus rechtlichen, politischen und zweckdienlichen Gründen²⁸ kaum durchführbar und wird einen Ausnahmefall bilden - im Unterschied zum privaten Bereich werden im öffentlichen Sektor internationale Datenverarbeitungssysteme zwischen nationalen Behörden sehr selten sein. Der internationale Informationsaustausch gewinnt aber auch bei militärischen Bündnissen verschiedener Länder²⁹ an Bedeutung; oder, wenn eine Nation innerhalb der Grenzen einer andern Daten systematisch zu nachrichtendienstlichen Zwecken sammelt.³⁰

3. Datenaustausch multi- und supranationaler Organisationen

Internationale Organisationen³¹ unterhalten mit ihren Mitgliedstaaten Datennetze oder Informationskanäle, mittels derer Daten aus den einzelnen Ländern - oft in anonymisierter und statistischer Form - exportiert werden, um der Organisation eine Konsolidierung der Informationen in den verschiedenen Fachbereichen zu ermöglichen. Gegenüber dem zwischenbehördlichen internationalen Datenaustausch gibt es im öffentlichen Bereich im Wirkungsfeld internationaler Organisationen und der diplomatischen Vertretungen einen grossen Informationsverkehr, dessen Besonderheit darin liegt, dass die Normen nationaler Datenschutzgesetze auf den grenzüberschreitenden Datenverkehr dieser Stellen nicht anwendbar sind, weil die internationalen Orga-

27 Ebenso HONDIUS, OECD Informatics Studies 10, S. 213.

28 Der zwischenbehördliche internationale Datenaustausch hat im allgemeinen noch ein zu geringes Ausmass, als dass er solche zwischenstaatlichen Projekte rechtfertigen würde.

29 Z.B. NATO: Vgl. Brüsseler NATO-Uebereinkommen über die Weitergabe technischer Informationen für Verteidigungszwecke von 1970.

30 Jede Nation wird aus legitimen Gründen der nationalen Sicherheit den Datenaustausch bzw. den Datenexport zu solchen Zwecken untersagen.

31 Z.B. INTERPOL, Statuten vom 13.6.1956, vgl. hinten, S. 109ff.; FAO (Welternährungsorganisation); WHO (Welt-Gesundheitsorganisation), vgl. Satzung vom 22.7.1946, Art. 61-65; UNO, vgl. Suchtgiftkonvention von 1961, Art. 18.

nisationen Rechtsgebilde sui generis³² darstellen und für Verfolgung und Ausübung ihres Zweckes rechtliche Immunität des Sitzstaates geniessen.³³

III. Folgerung

FORSTMOSER hat in seinem Referat³⁴ anlässlich des Symposiums "Computer und Privatsphäre"³⁵ festgestellt und begründet, "dass das Sammeln und Verwerten personenbezogener Informationen legitim und notwendig, vom Betroffenen erwünscht, aber auch problematisch ist."³⁶ Ich will an diesem Punkte anknüpfen und den Satz erweitern mit der Feststellung, dass heute³⁷ der Transfer von personenbezogenen Informationen und sensitiven Daten über die Landesgrenzen hinweg, legitim und notwendig, von den Betroffenen erwünscht ist, aber auch Probleme aufwirft, die einer Lösung bedürfen.

Die Notwendigkeit und Legitimität des Exportes von Daten (nicht nur personen-, sondern auch sachbezogener) ist eine Folge der zunehmenden wirtschaftlichen Verflechtungen der einzelnen Industrienationen und ihres Fortschrittes, ferner der Internationalisierung und damit verbundenen Entwicklung zwischenstaatlicher und supranationaler Organe. Diese internationale Zusammenarbeit und wachsende Interdependenz besteht im Rahmen des freien Welthandels nicht nur auf privatwirtschaftlicher, sondern ebenso auf öffentlicher und supranationaler Ebene. Der grenzüberschreitende Datenverkehr ist nicht mehr ein theoretisches Phänomen, er ist Wirklichkeit.

32 Extraterritorialer Status.

33 HONDIUS, OECD Informatics Studies 10, S. 217.

34 FORSTMOSER, Grundfragen und Lösungsmöglichkeiten, S. 31ff.

35 "Computer und Privatsphäre" der IBM Schweiz zur Klärung von Grundsatzfragen am 7./8.11.1977 in Zürich.

36 FORSTMOSER, Grundfragen und Lösungsmöglichkeiten, S. 34f.

37 SIMITIS, Schwierigkeiten, S. 9, Anm. 31: In Kanada werden nahezu drei Viertel der im Lande selbst benötigten Daten aus den Vereinigten Staaten importiert.

SCHUCAN, S. 44, Anm. 24; weiteres Beispiel in Anm. 25.

§ 2 PROBLEME DES PERSOENLICHKEITSSCHUTZES

Zur allgemeinen Problematik ¹ und den Gefahren ² des Datenschutzes schlechthin gesellen sich im grenzüberschreitenden Datenverkehr noch die Schwierigkeiten, die einer internationalen Informationsbeschaffung inhärent sind und sich aus dem Verlagern von personenbezogenen Daten in ein Land mit anderer Rechtsordnung, fremden Gesetzen, anderen Kulturen, fremder Sprache, unterschiedlichen Sitten und Auffassungen etc. ergeben. Diesen Problemen steht das einzelne Datensubjekt hilflos und verloren gegenüber, falls ihm nicht von der nationalen Rechtsordnung ³ Schutz seiner Persönlichkeit gewährt wird. Dabei ist unbestritten, dass die Verantwortlichkeit für den Schutz der Persönlichkeitsrechte und der Privatsphäre des einzelnen Menschen beim Staat, bzw. beim nationalen Gesetzgeber liegt.

Die Schwierigkeiten ergeben sich deshalb, weil das einheimische Recht nicht mehr auf Daten angewandt werden kann, die das Territorium des Landes verlassen haben. ⁴ Das grösste Unbehagen verursacht der grenzüberschreitende Datenverkehr den nationalen Regierungen infolge des Bewusstseins, dass hier der Schutz der Daten gegen Unregelmässigkeiten und Missbräuche viel schwieriger aufzubauen ist als im einheimischen Schutzsystem. Die Relevanz der für den nationalen Bereich erarbeiteten Prinzipien und Grundsätze sollte auch für den grenzüberschreitenden Datenverkehr gegeben sein, weil sie u.U. wieder in der Anwendung eines fremden nationalen materiellen Datenschutzes resultieren (wenn ein solches in Kraft steht), das ebenfalls mit den Prinzipien des Europarates ⁵ in Einklang stehen könnte.

1 Vgl. FORSTMOSER, Grundfragen und Lösungsmöglichkeiten, S. 34f.

2 Id., S. 35f.

3 In der Regel wird es das Land seines Wohnsitzes sein.

4 Territorialprinzip.

5 Vgl. Resolutionen (73) 22 und (74) 29, hinten S. 239.

Ich halte es nicht für sinnvoll, für den grenzüberschreitenden Datenverkehr grundsätzlich andere Prinzipien und Rechte (z.B. Individualrechte) als im nationalen Bereich aufzustellen: Spezielle, auf den grenzüberschreitenden Datenverkehr anwendbare Grundsätze sollten nur dann statuiert werden, wenn sie mit denjenigen des nationalen Bereiches nicht in Einklang zu bringen sind, oder wenn die Natur des internationalen Datenverkehrs zusätzliche Prinzipien erfordert.

Die ersten Probleme tauchen bei der Verwirklichung des Publizitätsgrundsatzes^{6 7} auf: Wie soll ein Betroffener sein Persönlichkeitsrecht wahren können, wenn er nicht weiss, ob und welche Daten zu seiner Person ins Ausland verlagert werden? Die grossen Distanzen, die das Rechtssubjekt von seinen Daten, die in ausländischen Dateien gespeichert oder verarbeitet werden, trennen, können auch zu Hindernissen in der Wahrnehmung der Kontrollrechte führen, auch wenn bekannt ist, wo sich die Daten befinden. Wie erhält das Individuum Auskunft bzw. Einsicht in die zu seiner Person gespeicherten Angaben? In welcher Sprache wird die Auskunft erteilt,^{8 9} und wie wird sichergestellt, dass das Einsichtsrecht durchgesetzt wird.¹⁰ Wie steht es mit der Kostenlast bei Auskünften im Ausland - gibt es national einheitliche Gebührentabellen, oder herrscht Tariffreiheit? Wie werden die andern Kontrollrechte, wie z.B. Berichtigungs- oder Löschungsrecht, durchgesetzt und verwirklicht? Die bei den Individualkontrollen¹¹ den Bürger direkt treffenden Probleme verdeutlichen die Schwierigkeiten der Verwirklichung fundamentaler Individualrechte beim grenzüberschreitenden Datenverkehr. Zusätzlich stellt sich die

6 Vgl. Europarats-Resolution (73) 22, Grundsatz 6 sowie Resolution (74) 29, Grundsatz 1 + 5.

7 Frage der Transparenz des grenzüberschreitenden Datenverkehrs.

8 Eine Frage, die auch in der mehrsprachigen Schweiz geklärt werden muss.

9 Wer trägt die möglichen Uebersetzungskosten, wenn ich meine Auskunft in Suaheli erhalte?

10 Z.B. mit Zeitspanne, innerhalb deren Auskunfterteilung, bzw. Antwort erfolgen muss.

11 Als Kontrolle durch das betroffene Datensubjekt; vgl. auch FORSTMOSER, Grundfragen und Lösungsmöglichkeiten, S. 49.

Frage des anwendbaren Rechts, die vor allem dann komplex werden kann, wenn die einzelnen Phasen der Datenverarbeitung in verschiedenen Ländern durchgeführt werden.¹²

Der Schutz, den der Staat seinem Bürger gewähren kann, lässt sich auf verschiedene Arten verwirklichen: Den wirksamsten Schutz wird sicherlich ein generelles Verbot der Datenausfuhr bewirken, während ein freier, unregelter Informationsfluss die Gefahr von Persönlichkeitsverletzungen durch unkontrollierte und unkontrollierbare Datenverlagerungen in sich schliesst. Innerhalb dieser beiden Extreme sind sämtliche Abstufungen möglich. Mit der Problematik des Schutzes der Daten im Ausland und dem Bestreben eines jeden Landes, die Datensubjekte¹³ vor missbräuchlicher Datenverarbeitung zu schützen, besteht eher die Tendenz zum Exportverbot als zur generellen Freigabe. Ein Exportverbot könnte aber erhebliche und gewichtige finanzielle und wirtschaftliche Nachteile für ein Land bedeuten: Ein stark vom Ausland abhängiges und wirtschaftlich eng mit andern Nationen verknüpftes Land, wie z.B. die Schweiz, kann es sich strukturell nicht leisten, ein generelles Ausfuhrverbot zu erlassen, will es nicht wirtschaftlich und politisch in eine ökonomische Isolation geraten.

Ebenso unmöglich ist das andere Extrem mit nur minimalen oder gar keinen Bestimmungen zum Schutz der Persönlichkeit und einem unkontrollierten freien Datenfluss. Dadurch wächst die Gefahr, plötzlich von einem "Datenvorhang" umschlossen zu sein. Dies kann sich derart manifestieren, dass umliegende Staaten oder wirtschaftlich verbundene Länder mit Datenschutzgesetzen den Export ins "schutzlose" Land generell verbieten, weil für die Personen, die sich im fraglichen Staat aufhalten oder dort ihren Wohnsitz haben, ein mangelnder Schutz ihrer Daten existiert. Theoretisch ist dies für die Schweiz bereits möglich: Das schwedische, norwegische und österreichische Datenschutzgesetz z.B. enthalten Bestimmungen, nach denen der Export von Daten be-

12 Vgl. hinten, S. 300ff.

13 Dazu sollten auch die im Lande wohnhaften Ausländer gezählt werden.

willigungspflichtig¹⁴ ist. Eine Genehmigung zur Uebermittlung personenbezogener Angaben zur Datenverarbeitung im Ausland wird nur erteilt, wenn im importierenden Staat vergleichbare Datenschutzgesetze oder -bestimmungen diese Informationen schützen, oder "wenn vertraglich sichergestellt wird, dass den Bedingungen des Datenschutzgesetzes auch bei der Verarbeitung im Ausland entsprochen wird."^{15 16}

Mit der Problematik des Schutzes der Daten im Ausland und dem Bestreben eines jeden Landes, die Rechtssubjekte vor missbräuchlicher Datenverarbeitung zu schützen, stellt sich auch die Frage nach der Exporterlaubnis von Daten. Mit einem solchen bewilligungspflichtigen Export "droht aber hier eine neue Art von Protektionismus",¹⁷ der alle auf den internationalen Informationsfluss angewiesenen Unternehmen behindern kann.¹⁸

14 Vgl. hinten, S. 133f.

15 STADLER, OeVD 11/1978 S. 9f.

16 So die Regelung des österreichischen Datenschutzgesetzes, das grundsätzlich eine Genehmigung der Datenschutzkommission für den Export der Daten ins Ausland verlangt, "ausser die Ueberlassung erfolgt in einem Staat, in dem ein dem österreichischen entsprechendes Datenschutzgesetz in Kraft steht (als solcher wird die Bundesrepublik Deutschland anzusehen sein) oder es handelt sich um Daten des Betroffenen selbst oder es ist in völkerrechtlichen Verträgen vorgesehen." (STADLER, ebenda, S. 8ff.).

17 STADLER, NZZ Nr. 266/1977.

18 PANTAGES/PIPE erwähnen den Fall der Firma Siemens AG, die im Zuge der Zentralisierung der Angaben ihrer weltweit verstreuten Angestellten ein Personalinformationssystem in München errichtete, dem 70 Gesellschaften aus 40 Ländern angeschlossen sind und Daten über jeden Arbeitnehmer und dessen Familie, seine Ausbildung und beruflichen Fähigkeiten gespeichert werden. Diese Angaben erleichtern der Firmenleitung die Koordination und Planung für Einsatz und Verschiebung von Führungskräften mit Berücksichtigung familiärer Umstände (wie z.B. Schulpflicht der Kinder), ferner ermöglichen sie statistische Auswertungen, interne Ausbildungsplanung etc. Die schwedische Datenschutzbehörde ("Datainspektionen" = Data Inspection Board [DIB]) verweigerte unter gewerkschaftlichen Einfluss der Siemens Niederlassung die Ausfuhrbewilligung dieser Personalangaben, erstens weil die Bundesrepublik Deutschland damals noch über kein Datenschutzgesetz verfügte (Entscheidung vom 13. 3. 1975) und zweitens wegen der Befürchtung, einen Präzedenzfall für die übrigen schwedischen Gesellschaften mit einer zentralen Datenverarbeitung im Ausland zu schaffen. Das DIB verwies hauptsächlich auf das Risiko, auf Datenbanken im Ausland Angaben zu einem grossen Teil der eigenen

Bei erlaubtem oder freiem Datenexport aber vermag der Schutz des die Daten exportierenden Landes dem Datensubjekt wenig zu helfen, weil der Schutz der Persönlichkeit von der Gesetzgebung desjenigen Landes gewährleistet sein muss, unter dessen Rechtshoheit die personenbezogenen Informationen beim grenzüberschreitenden Datenfluss treten oder sich bereits befinden. Wie wirksam dieser Schutz für die einzelne Person sein wird, hängt allein von der Rechtsordnung dieses neuen, die Information speichernden Landes ab.

Aus den potentiellen Reaktionen ¹⁹ bei einem Ungenügen an Vorschriften zum Schutz von personenbezogenen Daten durch Länder mit Datenschutzbestimmungen und aus einem genehmigten bzw. erlaubten Export personenbezogener Daten bei vergleichbaren Datenschutz-Standards im Importland, wird eine Wechselwirkung von Exportmöglichkeit und Gegenrecht i.S. von Datenschutzbestimmungen ersichtlich. Die Konsequenz dieser Wechselwirkung besteht darin, dass ein grenzüberschreitender Datenverkehr mit einem wirksamen Persönlichkeitsschutz sich nur dann frei entfalten kann, wenn zwischen den datenaustauschenden Nationen vergleichbare Datenschutzgesetze angewandt werden. Daraus folgt, dass der Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr nicht auf einzelstaatlicher Basis mit Exportverbot bzw. -genehmigung, sondern nur auf bilateraler oder multinationaler Ebene durch entsprechende Zusammenarbeit in der generellen Frage des Persönlichkeitsschutzes im Bereich des Datenschutzes gelöst werden kann. Isolierte einzelstaatliche Regelungen werden immer einen aus Persönlichkeitsschutz-Gründen erfolgenden protektionistischen Beigeschmack haben und in ihrer Bedeutung für einen weltweiten freien grenzüberschreitenden Datenverkehr mit wirkungsvollem Persönlichkeitsschutz hemmend sein.²⁰

Bevölkerung zu haben. (A New Headache for International DP, Datamation Nr. 6/1977, S. 118 und TDR, Vol. 1, No. 3, June 78, S. 4/6); vgl. auch VINGE, S. 58.

¹⁹ Z.B. in Form von Datensperren.

²⁰ Vgl. FREESE, Data Flow, S. 53ff.

§ 3 WIRTSCHAFTLICHE PROBLEME

Nebst den Problemen im Zusammenhang mit einer rechtlichen Regelung des Persönlichkeitsschutzes im grenzüberschreitenden Datenverkehr entstehen oder existieren bereits - infolge eines wachsenden internationalen Informationshandels mit dem lebenswichtigen "Rohstoff Information" - verschiedene wirtschaftliche Probleme, die teilweise den Interessen zum Schutz der Privatsphäre entgegenstehen und politische, sozialwirtschaftliche Themenkreise betreffen. (Man muss sich bewusst sein, dass der Datenschutz einen Eingriff in die Informationsflüsse und Datenverarbeitung darstellt und Auswirkungen auf die Wirtschaft hat.)

I. Beschäftigungsgrad¹

Die nationale Arbeitslosenquote kann von einer Regelung des grenzüberschreitenden Datenverkehrs zum Schutz der personenbezogenen Daten im positiven wie im negativen Sinne beeinflusst werden.

1. Positiv bezüglich des nationalen Beschäftigungsgrades ist die Wirkung einer protektionistischen Rechtswahl i.S. eines Exportverbotes, wenn das Ausland niedrigere Datenverarbeitungskosten² und Löhne³ hat, so dass die inländischen Firmen aus Kostengründen eine Verarbeitung ihrer Daten im Ausland vorziehen würden, dies aber einer rechtlich restriktiven Regelung wegen nicht tun können. Eine solche, die Verarbeitung personenbezogener Daten im Ausland hemmende oder gar verbietende Regelung trifft oft den Vorwurf eines verschleierte nationaler Protektionismus, da damit versucht werde, die Gesetze der freien Marktwirtschaft und des Weltmarktes zu korrigieren.

1 Vgl. FREESE, Data Flow, S. 46f.

2 Z.B. Umsatzsteuer, Mehrwertsteuer, Telefongebühren, Anschaffungskosten für DV-Anlagen, geringere Belastung durch weniger Datenschutz- und Datensicherungsvorschriften.

3 Beispiel USA - Kanada: Kanada hat höhere Löhne und Umsatzsteuern, so dass die Datenverarbeitungskosten in Kanada durchschnittlich 20% höher sind als in den USA.

In Kanada sollen z.B. durch den noch unregulierten Export von Daten und deren Verarbeitung in den USA 30'000 bis 40'000 Arbeitsplätze verloren gegangen sein.⁴ Solch ein Arbeitsplatzverlust wiegt umso schwerwiegender, als er im wachstumsfähigen Gebiet der Elektronikindustrie vorkommt; entsprechend gegensätzlich sind die Standpunkte: Arbeitnehmer und Gewerkschaften plädieren für eine rechtliche Regelung des grenzüberschreitenden Datenverkehrs, weil diese sich davon einen höheren Beschäftigungsgrad im Inland erhoffen, während die Wirtschaftsvertreter höhere Datenverarbeitungskosten und einen beschränkten Informationsfluss befürchten.

2. Negative Wirkung auf den Beschäftigungsgrad könnte eine restriktive Regelung verursachen, wenn wegen erhöhter Datenverarbeitungskosten oder verminderten wirtschaftlichen Informationspotentials, infolge erschwerter Datenexport bzw. -importmöglichkeiten, die Unternehmen mit einer Abwanderung ins Ausland reagierten, (oder die Unternehmenskosten beträchtlich steigen).

II. Zahlungsbilanzprobleme

Die Zahlungsbilanz kann gleicherweise durch das Fehlen resp. Vorhandensein einer Regelung des grenzüberschreitenden Datenverkehrs beeinflusst werden, da eine hohe Arbeitslosigkeit meistens (aber nicht zwingend) auch ein Zahlungsbilanzdefizit zur Folge hat. Der Import von im Ausland verarbeiteten Daten führt somit nicht nur zu einem Arbeitsplatzverlust, sondern auch zu einem steuerrechtlichen wie umsatzsteuermässigen Einnahmenausfall.^{5 6}

-
- 4 SERWATYNSKI, Information Privacy, Vol. 1, No. 2, S. 81; in: Vol. 1, No. 3, S. 134, vergleicht er den Fall mit dem "brain drain" von Kanada nach den USA während der Nachkriegsjahre.
 - 5 Für Kanada errechnete das Canadian Government's Department of Communications einen Einnahmenverlust von \$ 150-300 Millionen im Jahre 1976 (SERWATYNSKI, a.a.O.).
 - 6 STEINMUELLER, DVR 8/3 1979, S. 226.

III. Beeinflussung der einheimischen technologischen Entwicklung

Durch die Aufstellung von Einschränkungen im grenzüberschreitenden Datenverkehr befürchten viele Staaten eine Verlangsamung der technologischen Entwicklung im Inland. Diese kann einerseits dadurch verursacht werden, dass Daten nicht mehr routinemässig für eine hochstehende Verarbeitung ins Ausland transferiert werden können, wenn keine entsprechenden inländischen Verarbeitungsmöglichkeiten vorhanden sind; andererseits durch die Abwanderung von Firmen und den damit verbundenen Arbeitsplatzverlusten, die einen Rückgang an technologischer Intelligenz in einem wachstumssträchtigen und entwicklungsfähigen Gebiet mit sich bringen. Dies kann langfristig auch negative Auswirkungen auf eine einheimische Elektronikindustrie haben, weil technologisch fortgeschrittenere Erzeugnisse des Auslandes der einheimischen Produktion vorgezogen werden.

Diese wirtschaftlichen Folgen des grenzüberschreitenden Datenverkehrs sind ein - ohne protektionistischen Eingriff - nicht zu vermeidender negativer Effekt der freien Marktwirtschaft, der dem System inhärent und von verschiedenen Fällen bereits bekannt ist. Das Dilemma des Staates ist offensichtlich und die Problematik ambivalent: Bestrebungen von Regierungen, mit Hilfe von Einschränkungen des grenzüberschreitenden Datenverkehrs den wirtschaftlichen und sozialen Problemen eines Landes korrigierend zu Leibe zu rücken, sind dem eigentlichen Problem, dem Individuum auch im grenzüberschreitenden Informationsverkehr Schutz seiner Persönlichkeit zu gewähren, eher abträglich, da einzelstaatlicher Protektionismus im freien Wettbewerb Reaktionen provoziert. Der Zweck des Persönlichkeitsschutzes kann aber weder im nationalen noch im internationalen Bereich die Provokation von Handelspartnern oder Dritten sein.

§ 4 ABHAENGIGKEITSPROBLEME

Durch die unkontrollierte Verlagerung und Speicherung grosser, auf Individuen, Personengruppen und juristische Personen bezogener Datenmengen ins Ausland entsteht für manche Regierungen eine Problematik, die politisch weitreichender ist als die wirtschaftliche, weil sie die Nationalstaatlichkeit in ihrem Kern auf die verschiedensten Arten bedrohen kann und deren Verletzbarkeit erhöht. Ein Staat könnte deshalb versucht sein, diesen unerwünschten Wirkungen eines unregelmässigen Datenverkehrs unter dem Vorwand des Schutzes der Persönlichkeit im grenzüberschreitenden Datenverkehr präventiv entgegenzutreten. Der Persönlichkeitsschutz im internationalen Bereich sollte aber nicht dazu verwendet werden, gleichzeitig nationale Abhängigkeitsprobleme zu lösen. Diese neuartige Dependenzproblematik ist eine Folge der modernen Technologie, die ein wesentlicher Träger der Wirtschaftsordnung darstellt - eine Ueberbewertung dieses Problemkreises ist sicherlich falsch, weil die Abhängigkeit eine gegenseitige ist und damit teilweise neutralisierend wirkt.

I. Bedrohung der nationalen Sicherheit

Die Bedrohung der nationalen Sicherheit kann durch den Export von Daten gleichzeitig an mehreren Fronten erfolgen:

1. Mit zunehmendem Fluss sowohl personen- als auch sachbezogener Daten ins Ausland steigt die Abhängigkeit des datenexportierenden Landes von stabilen politischen Voraussetzungen und Bedingungen in den Datentransitländern und datenverarbeitenden Ländern.¹ Politische Unregelmässigkeiten in einem ausländischen Staat, der einheimische Daten befördert, verarbeitet oder speichert, können sicherheitspolitisch nachteilige Folgen für die nationale Sicherheit haben, da die Information als Schlüssel zur

1 Ebenso: SARBARHETSKOMMITEN, S. 9.

2 CARMODY, Information Privacy, Vol. 1, No. 1, S. 28.

Machterhaltung dient und Regierungen immer Mittel finden, mit denen sie sich nicht nur Informationen über Individuen des eigenen, sondern auch fremder Staaten beschaffen können, wenn sie es wollen.²

Als Nebeneffekt werden politisch stabile Nationen mit demokratischen Gebilden bevorzugt und um Stabilität ringende Länder der Dritten Welt gemieden, so dass diese neue Tendenz die Kluft zwischen Industrienationen und Entwicklungsländern vergrößern kann, indem sie datenreiche und datenarme Nationen schafft.³

2. Auch wenn die politischen Bedingungen in den Datentransit- und datenverarbeitenden Ländern stabil sind, besteht die Gefahr, dass die Daten eines Landes auf einer ausländischen Datenbank widerrechtlich angeeignet, manipuliert, zerstört oder auf andere Weise zum Nachteil des Datenursprungslandes verwendet werden können.⁴
3. Die Möglichkeiten nationaler Regierungen sind vermindert, im Ernstfall direkten Einfluss auf die Handlungen multinationaler Gesellschaften oder Institutionen auszuüben, wenn diese die lebenswichtigen Daten für ihre unternehmerischen Entscheidungen in ausländischen Zentralsystemen speichern.

II. Gefährdung der nationalen Souveränität⁵

Auf wirtschaftlichem Gebiet wird durch den grenzüberschreitenden Datenfluss eher eine wachsende Abhängigkeit als Unabhängigkeit ge-

3 Vgl. auch hinten, S. 37ff.

4 SERWATYNSKI erwähnt den Fall des General Accounting Office, das 38 Tapes mit Adressen von 1.14 Millionen Amerikanern vom US Social Security Administrations Zentralcomputer ohne deren Wissen entfernte. (Information Privacy, Vol. 1, No. 2, S. 81).

5 PIPE, Computerworld, 5/9/77, S. 5; SERWATYNSKI, Information Privacy, Vol. 1, No. 3, S. 81; vgl. ferner UNESCO/ IBI-Konferenz "Strategies and Policies for Informatics" (SPIN), TDR, Vol. 1, No. 6, S. 1/13.

schaffen. Durch die Verarbeitung von Wirtschaftsdaten im Ausland kann einer Nation ein grosser Teil lebenswichtiger Informationen verloren gehen, wenn nicht (mit erheblichem Kostenaufwand) sicherheitshalber eine Kopie der exportierten Daten im Inland gespeichert wird.⁶ Mit dem Verlust des Zugangs zu wichtigen Informationen wächst die Gefahr, dass industrielle und soziale Entwicklungen in einem Lande teilweise von Entscheidungen bestimmter Interessengruppen und einer Industrielobby von andern Ländern aus gesteuert werden, denen einzelstaatliche und binnenwirtschaftliche Probleme und Ueberlegungen nicht bekannt oder für sie irrelevant sind, weil primär ökonomische Erwägungen im Vordergrund stehen. Die in der Weltwirtschaft zunehmende Machtkonzentration, die innerhalb der multinationalen Gesellschaften durch Fusion, Erwerb oder Beteiligung an andern Unternehmen entsteht, verdeutlicht die immer grösser werdende potentielle Abhängigkeit von kleinen Interessengruppen, die bei verantwortungslosem Missbrauch ihrer Wirtschaftsmacht sogar die nationale Souveränität eines Staates ins Wanken bringen könnten.^{7 8 9}

6 Die Verletzbarkeit bleibt auch in der innerstaatlichen Datenverarbeitung ein Problem, vor allem kann bei einer Zentralisation von Daten ein Systemausfall verheerende Folgen zeitigen.

7 Dieser Extremfall ist m.E. nicht wahrscheinlich, da sich bei einer extremen Machtkonzentration immer ausgleichende Gegenkräfte bilden. Ebenfalls gegen eine Machtpolarisierung und Verletzbarkeit in dem oben (Anm. 6) erwähnten Ausmass spricht heute schon die Struktur von Datennetzen, die auf dem Prinzip des "distributed data processing" beruhen, so dass jeder einzelne Bereich seine eigenen Daten selbst verarbeitet, diese aber nur für eine globale Konsolidierung auf ein leistungsfähiges Zentralsystem verlagert, d.h. zur Beurteilung nationaler Ergebnisse wird nationale Datenverarbeitung betrieben; nur zur Konsolidierung auf internationaler Ebene werden die nationalen Ergebnisse über die Grenzen auf einen im Ausland stehenden Zentralcomputer übermittelt.

8 Vgl. auch STEINMUELLER, DVR 8/3 1979, S. 227 N 4.

9 Vgl. auch GOTLIEB/DALFEN/KATZ, S. 246f.: Hier wird auch die Bedrohung der sog. informationellen Souveränität erwähnt.

III. Gefährdung der nationalen Identität ¹⁰

Kaum sind die Zeiten der Entkolonialisierung und die letzten Ueberreste von nationalistischem Denken dem Europagedanken und/bzw. der allgemeinen internationalen Oeffnung resp. den Verständigungsbe-
mühungen gewichen, sind bedenklich stimmende, neue Schlagworte wie elektronische Kolonisation, elektronischer Imperialismus, Datenhege-
monie ¹¹ zu hören. Es gibt Personen, die bereits eine kulturelle Ueberschwemmung ¹² oder Vernichtung durch die technologisch dominan-
ten Nationen befürchten. Sie wollen nicht, dass ihre Wirtschaft, Banken, Behörden, soziale Struktur, Zeitschriften, Literatur, Musik und die übrigen Lebensaspekte "amerikanisiert" werden. Sie wollen aber ebensowenig "anglisiert, germanisiert, sowietisiert" oder auf andere Weise von einer fortgeschrittenen, frei über die Grenzen flies-
senden Informationstechnologie besiegt werden, so dass die eigene nationale Identität Gefahr läuft, ausgelöscht zu werden. ^{13 14 15 16}

10 SERWATYNSKI, Information Privacy, Vol. 1, No. 2, S. 81; vgl. auch TDR, Vol. 2, No. 5, S. 8.

11 CARROLL, S. 205.

12 LEMOINE beschreibt den kulturellen Effekt solcher Datenflüsse, der beträchtlich sein kann, wenn man bedenkt, was eine "Megasoftware" für Organisationsformen in Gesundheit, Erziehung oder Verkehrskontrolle zu bewirken vermag, wenn sie in Länder der dritten Welt exportiert werden soll. Ein Export höchster Technologien in Entwicklungsländer kann leicht zu einer "Ueberschwemmung" ausarten und nachteilige Folgen haben, da viele dieser Nationen noch nicht einmal den Schritt vom Agrarstaat zum Industriestaat vollzogen haben, von der westlichen Welt aber in einen Informationsstaat umgeformt werden; (TDR, Vol. 2, No. 1, S. 12).

13 EGER, Computerworld 13/2/1978, S. 15.

14 Dieses Denken ist m.E. gefährlich, weil es neuen Nährboden für Nationalismus und Völkerfeindschaften sein könnte. In einer Zeit der internationalen Oeffnung eines Weltwirtschaftsystems sollten die potentiellen Einflüsse anderer Nationen dem Aufbau einer neuen Weltinformationsordnung nicht entgegenstehen.

15 PANAGES/PIPE sprechen von Homogenisierung der Bürger eines Landes durch Speicherung auf internationalen Archiven (S. 118).

16 GOTLIEB/DALFEN/KATZ (S. 247f.) sprechen von einer Gefährdung der kulturellen Identität.

IV. Der politische Aspekt: Dritte Welt und Entwicklungsländer ¹⁷

Der Informationsverkehr wird durch die internationale Ausweitung auch die Entwicklungsländer erfassen und kann deren Bestrebungen, die Kluft des wirtschaftlichen und technischen Standes gegenüber den Industriestaaten zu verringern, torpedieren. Vergrößert wird der Unterschied, wenn Entwicklungsländer einerseits wegen politischer Unrast der gezielten Einführung von Datenverarbeitung im eigenen Lande keine Bedeutung zumessen oder andererseits durch ungeplanten Einsatz eine Ueberschwemmung mit neuer Technologie ¹⁸ erfolgt, die eine kulturelle Gegenreaktion auslösen könnte. Verkleinert wird die Kluft, wenn die Anwendung von Datenverarbeitungssystemen ausgewogen und gezielt zur Steigerung eines stagnierenden oder langsamen Wachstums benutzt wird. Die technologisch hochstehenden Industriestaaten und die Hersteller von Datenverarbeitungssystemen müssen sich beim Aufbau eines Weltinformationsnetzes der Probleme der Entwicklungsländer bewusst und ihnen bei der Lösung der Problemvielfalt ¹⁹ behilflich sein. ²⁰ Abhängigkeit sollte hier zu einem Hilfe- und Ausbildungsstimulans genutzt werden, indem diesen Nationen:

- Hilfe bei der Definition und Erarbeitung einer generellen Datenverarbeitungs- bzw. Informationspolitik in Uebereinstimmung mit den nationalen Plänen geboten,

17 Vgl. auch die von UNESCO und IBI (Intergovernmental Bureau for Informatics) veranstaltete zwischenstaatliche Konferenz "Strategies and Policies for Informatics" (SPIN) von Malaga/Torremolinos im August 1978 und deren Resolutionen, die hauptsächlich die Probleme der dritten Welt widerspiegeln; ferner Ergebnisse der IBI World Conference on Transborder Data Flow Policies vom 23.-27. Juni 1980 in Rom: vgl. DS+DS 4/80, S. 240.

18 Vgl. vorne, Anm. 12, S. 20.

19 Z.B. - ungenügend qualifiziertes Personal;
- ungenügend praktische Erfahrung;
- fehlende Festsetzung von Basisvorgehen zur Lösung von EDV-Problemen;
- fehlende effiziente Entwicklungspolitik;
- mangelnde Planung mit genereller wirtschaftlicher Entwicklung usw.

20 Lomé-II vom November 1979 ist ein erster Schritt in dieser Richtung.

- Unterstützung bei der Einführung eines effektiven Planes für den sinnvollen und kontrollierten Einsatz von Computertechnologie gewährt,
- ein freier Zugang zu technologischen Informationen der Industriestaaten sichergestellt ²¹ und
- die Frage der Abhängigkeit von multinationalen Informationsnetzen und von ausländischer EDV-Versorgung geklärt wird.

Andererseits sind auch Zusammenarbeitsverträge ²² von Entwicklungsländern untereinander bedeutsam, da sie oft eine gleichlautende Problemstellung in Kooperation zu lösen vermögen.

20 Vgl. UNESCO/IBI: SPIN-Conference, Recommendations 32.4 und 10.

21 Z.B. vereinbarten Algerien und Rumänien am 11.5.1977 einen solchen Zusammenarbeitsvertrag.

§ 5 DER GRENZUEBERSCHREITENDE DATENVERKEHR IM SPANNUNGSVERHAELTNIS
ZWISCHEN FREIEM INFORMATIONSFLUSS UND SCHUTZ PERSONENBEZOGENER
DATEN

Es ist notwendig, einen Ausgleich und eine Lösung der entgegengesetzten Interessen, nämlich einerseits am Schutz der Privatsphäre und andererseits an einem ungehinderten Datenfluss mit Informationsfreiheit, anzustreben, damit die Möglichkeiten der modernen Datenverarbeitungstechnologie voll ausgeschöpft werden können, soweit dies wünschbar ist. Ausserdem sollte die technologische Innovation nicht durch rechtliche Hindernisse paralysiert werden.

I. Prinzip des freien Datenflusses

Die Bedeutung eines freien Informationsflusses auf nationaler und internationaler Ebene ist vor allem im wirtschaftlichen Bereich in seinen Ausmassen erkennbar. Innerhalb der heutigen Wirtschaftsordnung ist ein ungehemmter, innerstaatlicher wie grenzüberschreitender Fluss sach- und personenbezogener Daten zur Erfüllung von Verträgen, Dienstleistungen, gesetzlichen Vorschriften und geschäftlichen Angelegenheiten sowie der regelmässigen Kommunikation zwischen Organisationen, ökonomischen Regionalsystemen und ihren Mitgliedern von gleicher Wichtigkeit wie für das Funktionieren des freien Handels und des Weltwirtschaftsystems.

Der freie Informationsfluss muss deshalb sowohl von den Regierungen als auch vom internationalen Recht im grösstmöglichen Ausmass garantiert werden, mit der allseitigen Zusicherung, dass beständige, ungehemmte Flüsse ausländischer Daten respektiert werden. Die Fähigkeit der Länder, einen ununterbrochenen Fluss von Informationen zu gewährleisten, ist von vielen Faktoren abhängig, hauptsächlich aber von der verfassungsmässigen und gesetzlichen Macht einer Regierung und ihrem Verständnis, einen massvollen Ausgleich zwischen nationalstaatlichen Interessen und dem der internationalen Wirtschaft und Kooperation zu finden.

II. Einschränkungen des Datenflusses

Das Prinzip des freien nationalen und internationalen Informationsflusses muss aber aus verschiedenen Gründen relativiert werden.

1. Das legitime Interesse eines Staates, den Austausch solcher Informationen zu untersagen, die die nationale Sicherheit ¹ betreffen, im Widerspruch zu innerstaatlichen Gesetzen, der gesamten Rechtsordnung bzw. des "ordre public" stehen oder Rechte seiner Einwohner bzw. Aufenthalter ² verletzen. Als relevantester Einschränkungsfaktor des freien grenzüberschreitenden Datenflusses gilt der Schutz der Persönlichkeit, deren Verletzung durch Missbrauch personenbezogener Angaben verhindert werden muss.

Lösungen dieser Probleme, die in einer Korrektur des freien Wettbewerbs resultieren, um Arbeitsplätze zu sichern, bessere Zahlungsbilanzen zu erhalten, die eigene Datenverarbeitungsindustrie zu fördern und nationale Eigenart gegen fremde Einflüsse etc. zu schützen, sind Systeme des Datenprotektionismus, die sich schädlich auf die zwischenstaatlichen Beziehungen und langfristig auch auf die gesamte Wirtschaftslage auswirken können.³

Bestehende protektionistische bzw. einen freien Austausch verhindernde Bestimmungen einer nationalen Rechtsordnung müssen ebenfalls überprüft und, wenn notwendig, revidiert werden.⁴

Auf dieser Relativierungsstufe sollten sich die einzelnen Staaten zu einem möglichst grossen Spektrum des Informationsverkehrs und

1 Die Definition, welche Daten die nationale Sicherheit betreffen, ist eine souveräne Entscheidung jedes Landes, sollte aber nicht extensiv ausgelegt werden (vgl. vorne, S. 17f.) damit keine derartig getarnten protektionistischen Massnahmen den freien Fluss begrenzen; hier wären Richtlinien einer internationalen Organisation sehr wünschenswert.

2 Auch Ausländer, die sich im betreffenden Staat aufhalten.

3 Datenschutzgesetze dürfen den erforderlichen Informationsaustausch im Interesse eines freien und fairen Welthandels nicht belasten.

4 Z.B. Art. 273 StGB, vgl. hinten, S. 383ff.

seiner Arten bekennen und Einschränkungen nur zum Schutz der Persönlichkeit gegen Missbrauch personenbezogener Informationen und in andern speziellen Fällen mit anerkannten Gründen vornehmen.

2. Die supranationalen Bestrebungen mehrerer Staaten, ihre legitimen einzelstaatlichen Interessen gegenüber einem Rechtsvakuum und damit schrankenlosem Gebrauch bzw. potentielltem Missbrauch zu schützen. Die Entstehung von "data havens" (i.S. von datenschutzlosen Räumen) kann nur mit der Einschränkung des freien Datenflusses durch das Kollektiv verwirklicht werden. Dies hat zur Folge, dass ein freier Datenfluss, - vorausgesetzt, man negiert Datenoasen grundsätzlich - nicht absolut gefordert werden kann, sondern nur innerhalb des Kollektivs, das mittels einer internationalen Konvention oder eines Vertrages in allen Mitgliedstaaten minimale und untereinander anerkannte Datenschutz-Standards garantiert, damit der freie Datenfluss innerhalb dieses Kollektivs ungehindert läuft.

Die logische Folge der Verwirklichung eines freien Datenflusses in einem möglichst grossen Umfang und einem wirksamen Persönlichkeitsschutz im internationalen Bereich resultiert m.E. in einem Vertragsabschluss auf supranationaler Ebene.

Im folgenden sollen die eine internationale Lösung des grenzüberschreitenden Datenverkehrs beeinflussenden nationalen und internationalen Regelungen der beiden Antagonisten betrachtet werden.

III. Persönlichkeitsschutz

1. National

Jede Rechtsordnung enthält in ihrem öffentlich- wie privatrechtlichen Gesetzesbereich Bestimmungen zum Schutz der Persönlichkeit; teilweise beruht das Recht auf Persönlichkeit und dessen Schutz auf verfassungsrechtlicher Grundlage.^{5 6} Die Ausgestaltung des Persön-

5 BRD: Art. 1 und 2 GG.

lichkeitsschutzes ist von Land zu Land unterschiedlich. Bei der Rechtsvergleichung einiger wichtiger Institutionen der Regelung des Persönlichkeitsschutzes wird die vielen Gesetzgebungen gemeinsame Schwierigkeit offenbar, eine klare Begriffsbestimmung und Abgrenzung des Persönlichkeitsrechts zu geben. Auffallend ist, dass nirgends eine befriedigende Unterscheidung der Rechtsbegriffe Person und Persönlichkeit getroffen werden kann, sondern teils als Synonyme, teils als differenzierte Begriffe verwendet werden. Die Schwierigkeit einer klaren Definition liegt letzten Endes in der Komplexität des menschlichen Individuums.

Im schweizerischen, deutschen, französischen, österreichischen und andern nationalen Rechtskreisen des Kontinents hat das Persönlichkeitsrecht überall die gleiche Grundstruktur: "Die nationalen Unterschiede sind nicht qualitativer, sondern bloss quantitativer Natur, d.h. verschieden ist die Formulierung, das Ausmass der geschützten Güter, nicht aber der Grundgedanke und die grundlegende Methode des Schutzes."⁷ Zu dieser Parallelität der grundlegenden Methoden des Persönlichkeitsschutzes kommt noch eine gewisse Homogenität der Mittel bei den bisher in Europa erlassenen Datenschutzgesetzen und -entwürfen. Diese singuläre Erscheinung beruht einerseits auf den Grundsätzen der Resolutionen (73) 22 und (74) 29 des Europarates, die in empfehlender Form eine Reihe von Datenschutzgrundsätzen enthalten, andererseits ergibt sie sich aus der Natur der Sache, d.h. der Datenverarbeitung, die überall auf den gleichen Prinzipien beruht. Der heutige internationale Standard, der durch "Befolgung" dieser Reihe von Grundsätzen erreicht wurde, ist nicht aus nationalen Rechtsordnungen herangewachsen, sondern dem Weitblick und der Initiative internationaler Organisationen zu verdanken.⁸

6 Die schweizerische Rechtsordnung hat in der bundesgerichtlichen Rechtsprechung (BGE 89 I 98, 97 I 49, 98 Ia 423, 102 Ia 282, 105 Ia 29) die Rechte der Einzelperson, die mit den Freiheitsrechten der Verfassung in naher Beziehung stehen, als "ungeschriebene Verfassungsrechte" anerkannt, so z.B. die persönliche Freiheit.

7 BUCHER, S. 65.

8 Vor allem Europarat und OECD.

2. International

Auf internationaler Basis enthält vor allem:

- A. Die europäische Menschenrechtskonvention in Art. 8 eine den Persönlichkeitsschutz betreffende Rechtsnorm und gewährt dem Individuum "Anspruch und Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."⁹ "Das Recht auf Achtung des Privatlebens entspricht dem Recht auf Achtung der Intimsphäre, deren Schutz als Teil des allgemeinen Persönlichkeitsrechts abgeleitet wird."¹⁰ Dieser in Art. 8 verwirklichte Persönlichkeitsschutz ist aber rein öffentlich-rechtlicher Natur und schützt die Individuen nur vor Eingriffen des Staates, so dass Art. 8 bei Verletzungen von Rechtsgütern durch Private oder Presse nicht anwendbar ist. Die Rechtsträger sind teilweise nur natürliche Personen: so beim Privat- und Familienleben; bei der Wohnung und beim Briefverkehr hingegen sind sowohl natürliche wie juristische Personen¹¹ des Zivilrechts Träger des Grundrechts. Juristische Personen des öffentlichen Rechts sind als Rechtsträger ausgeschlossen, weil der Staat sich nicht selbst vor staatlichen Eingriffen schützen kann.
- B. Die Allgemeine Erklärung der Menschenrechte¹² von 1948 ist mit ihrem Art. 12 ebenso wie
- C. Der Internationale Pakt über bürgerliche und politische Rechte der Vereinten Nationen vom 19.12.1966¹³ in seiner Formulierung des Art. 17 dem Wortlaut des Art. 8 der EMRK sehr ähnlich und ebenfalls nur öffentlich-rechtlicher Natur.

9 AS 1974 II, S. 2151ff.

10 GURADZE, S. 118.

11 in- und ausländische Personen.

12 SARTORIUS II, vgl. Nr. 19: Allgemeine Erklärung der Menschenrechte der Vereinten Nationen vom 10. Dez. 1948.

13 SARTORIUS II, vgl. Nr. 20: Internationaler Pakt über bürgerliche und politische Rechte der Vereinten Nationen vom 19.12.1966.

- D. Auf zivilrechtlicher Ebene gibt es im internationalen Bereich keine rechtssetzenden Normen zum Schutze der Persönlichkeit. Nur die Resolution (73) 22 des Europarates zum Schutz der Privatsphäre gegenüber elektronischen Datenbanken steckt den Rahmen des zivilrechtlichen Persönlichkeitsschutzes ab, die Resolution (74) 29 regelt ebenfalls den öffentlichen Bereich.

IV. Informationsfreiheit

1. National

Als national geschütztes Rechtsgut resultiert die Informationsfreiheit einerseits aus der verfassungsmässigen garantierten Meinungsäusserungsfreiheit: Informationsfreiheit im reflexiven Sinne, d.h. die Freiheit der Mitteilung setzt einen Empfänger voraus, dessen Recht ebenso geschützt werden muss;¹⁴ andererseits ist sie ein Rechtsgut des allgemeinen Persönlichkeitsrechts und kann unter den Schutz der Verhaltens- und Betätigungsfreiheit subsumiert werden.¹⁵ Die Schranken dieser Informationsfreiheit werden dementsprechend durch das Persönlichkeitsrecht eines andern und durch das Legalitätsprinzip des öffentlichen Bereiches gesetzt.

In neuester Zeit ist eine Tendenz auf zunehmende Informationsfreiheit des Bürgers gegenüber dem Staate zu beobachten,¹⁶ vor allem im Zusammenhang mit der Etablierung von Rechten bei der Datenverarbeitung im öffentlichen Bereich.

2. International¹⁷

Auf internationaler Ebene gibt es einige Verträge, die die freie Verbreitung von Informationen zum Ziele haben:

14 GURADZE, S. 143.

15 HOTZ, S. 39ff.

16 Vgl. EMRK, Art. 10; ferner den Entwurf für Totalrevision der schweizerischen Bundesverfassung vom 23.2.1978, Art. 7 und 12.

17 Vgl. auch ENGELHARD, S. 112f.

A. Europäische Menschenrechtskonvention vom 4.11.1950.

Als international geschütztes Rechtsgut ist die Informationsfreiheit in Art. 10 EMRK verankert und garantiert jedermann das Recht auf freie Meinungsäusserung, die auch die "aktive Informationsfreiheit"¹⁸ einschliesst, d.h. "die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen."¹⁹ Sie steht sowohl in- als auch ausländischen, natürlichen wie juristischen Personen zu. Einschränkungen der Informationsfreiheit erfolgen im Interesse der nationalen Sicherheit, der territorialen Unversehrtheit oder öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung und Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufes oder der gesetzlich vorgesehenen Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Angaben bzw. zur Gewährleistung der unparteilichen Rechtsprechung.²⁰

Die Informationsfreiheit nach Art. 10 EMRK steht aber nicht im Widerspruch zu dem in Art. 8 EMRK verankerten Recht auf Achtung der Privat- und Intimsphäre, da in Art. 10 Abs. 2 eine Beschränkung der Informationsfreiheit über vertrauliche Angaben zur Wahrung der Rechte Dritter erlaubt ist.

B. Internationaler Pakt über bürgerliche und politische Rechte der Vereinten Nationen vom 19.12.1966.

In Art. 19 ist das Recht auf Informationsfreiheit in einer der EMRK ähnlichen Formulierung festgelegt: "Jedermann hat das Recht auf freie Meinungsäusserung; dieses Recht schliesst die Freiheit ein, ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere Mittel eigener Wahl sich zu beschaffen, zu empfangen und weiterzugeben."²¹

¹⁸ GURADZE, S. 142.

¹⁹ AS 1974 II S. 2151ff.

²⁰ Vgl. Art. 10 Abs. 2 EMRK.

²¹ MALLMANN, International Agreements, S. 7, N 22.

C. Konferenz über Sicherheit und Zusammenarbeit in Europa (KSZE)
in Helsinki vom 1.8.1975.

In der Schlussakte²² der KSZE-Konferenz sind ausführliche Bestimmungen über Zusammenarbeit auf dem Gebiete des Informationswesens enthalten, mit der Zielsetzung, eine freiere und umfassendere Verbreitung aller Arten von Informationen zu erleichtern, die Zusammenarbeit im Informationsbereich und den Informationsaustausch mit andern Ländern zu fördern. Das Hauptgewicht dieser Bestimmung über das Informationswesen wird auf die Massenmedien bezogen, wobei die generelle Bedeutung eines freien Informationsflusses von den Teilnehmerstaaten anerkannt wird.

D. Ausserdem gibt es eine Anzahl von Verträgen,²³ die die zwischenstaatliche Kooperation in bestimmten Angelegenheiten des Informationssektors bezwecken und in einem Austausch von sach- und personenbezogenen Daten bestehen.

V. Bedeutung dieser internationalen Abkommen für den grenzüberschreitenden Datenverkehr

Gemeinsamkeit besteht bei all den aufgeführten internationalen Abkommen darin, dass sie ganz allgemeine und generelle Bestimmungen über die Informationsfreiheit und den Austausch bestimmter Arten von Daten enthalten, aber generell nicht auf die technischen Methoden der

22 KSZE, Phraseologie der KSZE-Schlussakte, vgl. Nr. 0711, 0726 und 0729.

23 Z.B. - Europäisches Uebereinkommen über die Rechtshilfe in Strafsachen vom 20.4.1959: v.a. Art. 13, 21, 22;
- Statuten der INTERPOL vom 13.6.1956;
- Haager Uebereinkommen betreffend Zustellung gerichtlicher und aussergerichtlicher Urkunden in bürgerlichen Rechts- und Handelssachen im Ausland vom 15.11.1965;
- Haager Uebereinkommen über die Beweisaufnahme im Ausland in Zivil- und Handelssachen vom 18.3.1970.

Uebermittlung eingehen und aus "Altersgründen"²⁴ den freien Informationsfluss im grenzüberschreitenden Verkehr sach- und personenbezogener Daten nicht behandeln können. Die Verträge werden Einfluss auf künftige internationale Regelungen des grenzüberschreitenden Datenverkehrs haben.²⁵

Der Schlussakte von Helsinki ist m.E. nicht allzuviel Bedeutung bezüglich eines freien Informations- i.S. eines Datenflusses, als Ausdruck der Informationsfreiheit, beizumessen. Helsinki war mehr ein politischer Akt im Kontext der Entspannungspolitik von Ost und West mit den entsprechenden positiven Auswirkungen auf die Massenmedien im Zusammenhang mit der Informationsfreiheit.

Der UNO-Weltpakt und die EMRK enthalten bedeutend konkretere Angaben zur Informationsfreiheit als reflexivem Recht der Meinungsäusserungsfreiheit. Sie basieren hauptsächlich auf Menschenrechten mit dem Schutz der Persönlichkeit vor Eingriffen des Staates und der freien Informationsverbreitung als einige der Ziele. Im UNO-Weltpakt wird konkret die Information in Schrift oder Druckform erwähnt und mit dem generalklauselartigen Begriff "andere Mittel eigener Wahl" die Palette der Möglichkeiten zur Informationsbeschaffung offengehalten, so dass darunter auch die elektronische Uebermittlung und der Empfang von Daten subsumiert werden kann.

Auffallend ist, dass die den Persönlichkeitsschutz regelnden Abkommen die Personen immer nur vor Eingriffen des Staates schützen: sie reflektieren damit die Wichtigkeit des öffentlichrechtlichen Schutzbereiches vor staatlicher Allmacht. Im Hinblick auf eine Lösung der Interessengegensätze (von Datenschutz und Informationsfreiheit), in einer diesen Abkommen adäquaten internationalen Konvention, müsste aber auch der zivilrechtliche Persönlichkeitsschutz integriert wer-

24 Der Ruf nach einem freien Datenfluss über die nationalen Grenzen hinweg tauchte erst gegen Mitte der 70er Jahre, als Folge der sich abzeichnenden Restriktionen im grenzüberschreitenden Datenverkehr durch einzelne nationale Datenschutzgesetze und Entwürfe, auf.

25 MALLMANN, International Agreements, S. 12, N 44.

den, da die Tätigkeit im grenzüberschreitenden Datenverkehr hauptsächlich von privaten Gesellschaften ausgeführt wird und den Individuen von diesem Bereich auch die meisten Verletzungsmöglichkeiten drohen. Im öffentlichen Sektor sind bereits eine gewisse internationale Zusammenarbeit und dadurch bedingte transnationale Datenflüsse zu finden, doch sind sie weder so häufig noch volumenmässig so ausgedehnt wie im privaten Bereich, da das Legalitätsprinzip der Verwaltung meist zwischenstaatliche Verträge als Rechtsgrundlage für eine behördliche Zusammenarbeit erfordert.

In der Schweiz wird die Europäische Menschenrechtskonvention die Regelung dieser beiden gegensätzlichen Interessenpaare im grenzüberschreitenden Datenverkehr beeinflussen.

§ 6 DATA HAVENS

I. Der Begriff

Der Begriff "data havens" - im Deutschen auch "Datenoasen" genannt - ist eine terminologische Nachbildung von "tax havens"¹ bzw. "Steuerparadiesen" und hat im Zusammenhang mit Datenschutz noch keinen fest abgegrenzten Inhalt und keine klare Definition erfahren.

Angesichts dieses noch weiten Definitionsspektrums unterscheidet WITTKAEMPER² zwischen:

1. Datenparadiesen im nationalen Sinne, die dadurch entstehen, dass der Gesetzgeber bewusst und gewollt Datenfreiräume schafft, z.B. durch Einschränkung des Anwendungsbereiches, so dass gewisse Datensammlungen, Verfahren und bestimmte Bereiche nicht vom Gesetz erfasst werden, und
2. Datenparadiesen im grenzüberschreitenden Sinne, die er umschreibt als "Ergebnis von nicht bewusst oder gewollt in Kauf genommenen Entwicklungen, sondern von Entwicklungsunterschieden im Bereich der Datenschutz und Datensicherheitsgesetzgebung".³

Die von WITTKAEMPER gewählte Unterscheidung ist m.E. nicht notwendig, da bei diesem Begriff sowohl die bewusste Schaffung von Datenfreiräumen durch einen Gesetzgeber als auch deren Berücksichtigung im internationalen Verkehr verstanden werden; diese Unterscheidung kann

1 "Tax havens" sind in jüngster Zeit aufgrund der internationalen Öffnung sehr zahlreich entstanden und charakterisieren sich oft als kleine, erst kürzlich selbständig gewordene Länder mit wenig natürlichen Quellen oder einheimischem Reichtum. Viele von diesen Kleinstaaten sind vor kurzem aus der Kolonialherrschaft entlassen worden, oder sind innerhalb derer autonom, d.h. sie erhalten keine finanzielle Hilfe des Mutterlandes mehr und sind auf eigene Einkünfte angewiesen, so dass sie als einzige Einnahmequelle den Tourismus oder die Steuerparadiesgeschäfte haben.

2 WITTKAEMPER, DS+DS 2/78, S. 59.

3 Id., a.a.O.

höchstens Anlass zur Verwirrung geben. Die Unterscheidung der "Daten-oasen im grenzüberschreitenden Sinne" ist zu eng.

Unter "data haven" ist allgemein jede Abweichung der Regelungsintensität und -dichte von einem Mittelwert an Datenschutznormen bzw. -ordnungen zu verstehen. Diese Abweichung kann in zwei gegensätzlichen Richtungen erfolgen, die zu verschiedenen Typen von "data havens" führen:

- Abweichung nach oben, d.h. i.S. eines besonders rigorosen und restriktiven Datenschutzrechts mit optimalem Schutz der Persönlichkeit.
- Abweichung nach unten, d.h. i.S. einer weitgehenden oder totalen Absenz von Datenschutznormen, die in einem mangelhaften oder keinem Persönlichkeitsschutz resultieren.

Beide Ausprägungsformen von "data havens" vermögen Daten zu attrahieren oder auszusperren. Die Attraktivität bzw. Negation eines Landes für Datenverarbeitung bzw. -speicherung gegenüber Dritten folgt nicht nur aus Entwicklungsunterschieden von Datenschutzgesetzgebungen, sondern aus dem Kontext der jeweiligen gesamten nationalen Rechtsordnung und Rechtsprechung, in der ein oder kein Datenschutzgesetz steht.⁴

In den folgenden Ausführungen dieser Arbeit wird unter dem Begriff "data haven" aber immer nur - in Übereinstimmung mit der terminologischen Nachbildung - die nach unten abweichende Form i.S. eines datenschutzarmen Raumes verstanden. Wo die gegenteilige Ausprägungsform i.S. einer restriktiven Datenschutz- und Rechtsordnung gemeint ist, wird dies speziell hervorgehoben.

II. Gefahren beim grenzüberschreitenden Datenverkehr

WITTKAEMPER⁵ nennt drei Hauptgefahren bei der Uebermittlung personenbezogener Daten in "data havens":

1. die Gefahr der Umgehung des nationalen oder regionalen Rechts oder Umgehung nationaler oder regionaler Kontrollsysteme,

⁴ Vgl. hinten V, S. 37.

⁵ WITTKAEMPER, a.a.O.

2. die Gefahr der Fehlbewertung, zweckwidrigen Benutzung und Manipulation personenbezogener Daten,
3. die Gefahr der Einschränkung oder sogar Aufhebung der Rechte des Betroffenen, da er sie entweder gar nicht oder nur theoretisch gegenüber dem eigentlichen Datenverarbeiter durchsetzen kann.

All diese Gefahren weisen eindeutig auf eine Umgehung,⁶ Unterwanderung und Aushöhlung der betreffenden nationalen Rechtsordnung hin, die alle nationalen Bemühungen und Verwirklichungen des Persönlichkeitsschutzes in einem freien Informationsfluss zu zerschlagen vermögen.

Diese Gefahren erhalten eine neue Dimension und Evidenz durch die bestehende Abhängigkeit ökonomischer Regionalsysteme von ihren Informations- und Kommunikationsstrukturen. So kann das Problem der "data havens"-Bildung ohne gemeinsame Schritte aller Staaten zu einer Schliessung der nationalen Informations- und Kommunikationsräume führen und den z.B. innerhalb der EG angestrebten Zielen einer europäischen Informations- und Kommunikationsgemeinschaft kontraproduktiv sein und damit in krassem Widerspruch zu dem durch die Gemeinschaft verfolgten Zweck stehen, der unter den Mitgliedstaaten einen Datenfluss voraussetzt. Eine Beschränkung des Datenflusses innerhalb der EG zum Schutz nationaler Datenbestände wirkt protektionistisch und steht im Widerspruch zu allen Absichten der europäischen Integration.⁷ Einzelstaatliche Datensperren werden deshalb nicht zur Lösung

6 Das American Council on Education machte eine Studie über Gewohnheiten, Sitten und Lebensstil junger Menschen in den USA und sammelte eine Reihe sensibler Informationen, die z.T. Angaben über illegalen (nicht medizinischen) Gebrauch von Drogen enthielten. Ein Entschlüsselungsband, das die in anonymer Form gespeicherten Daten auf die befragten Personen angewandt, sie wieder identifizierbar machen könnte, wurde in Kanada aufbewahrt, um es vor möglichen Strafandrohungen des Obersten Gerichtshofes der USA sicherzuhalten (CARROLL, S. 204f., mit weiteren Beispielen). Vgl. ferner Pressemitteilung von INTERTECT, in: Information Privacy, Vol.1, No.1, S. 9 und SIMITIS, Festschrift, S. 358, Anm. 8.

7 WITTKAEMPER, S. 60.

dieser Gefahren beitragen; sie können m.E. nur mit internationaler Zusammenarbeit zur Harmonisierung von Datenschutzgesetzen, multinationalen Verträgen oder einer internationalen Konvention⁸ geklärt werden.

III. Ursache von "data havens"

Ursache von Datenoasen sind ungleiche Rechtsordnungen und unterschiedliche finanzielle Lasten im Kommunikationsverkehr, die sich als Datenbarrieren manifestieren:

1. Nicht tarifliche Datenhindernisse können nationale Rechtsordnungen und Gesetzgebungen (ebenso fehlende Gesetze), aber auch bilaterale oder multilaterale Verträge, Verträge durch internationale Organisationen, unstabile politische Situation, geographische Lage u.a. sein.
2. Tarifliche Datenhindernisse sind hohe Uebermittlungskosten beim Kommunikationsverkehr,⁹ die einen Datenaustausch einzudämmen vermögen; hohe Steuerlasten, hohe Lebenskosten, hohe Importzölle auf technischem Material u.ä.

IV. Technische Voraussetzungen für "data havens"¹⁰

Datenoasen benötigen gute nationale Fernmeldeeinrichtungen, internationale Informations- und Kommunikationsstrukturen, eine verlässliche und abgesicherte Energieversorgung, aber ebenso eine unternehmensfreundliche und verantwortungsbewusste Regierung, die für eine stabile politische und wirtschaftliche Lage ihres Landes besorgt ist. Bevorzugt wird eine für die Kommunikation mit den grossen Industrie-

⁸ Vgl. hinten, § 14, S. 390ff.

⁹ Ebenso, ungleiche Gebühren der Uebermittlungsträger: z.B. verlangen die amerikanischen Telephongesellschaften für einen Zugriff auf englische Datenbanken mehr (12 \$ pro 64000 bytes), als die englische PTT für einen Zugriff auf US-Datenbanken (8 \$ pro 64000 bytes); ferner herrschen Unterschiede zwischen den internen und externen Ansätzen von amerikanischen Datenbanken und von Euronet (vgl. TDR, Vol. 2, No. 1, S. 4).

¹⁰ NORMANN, Information Privacy, Vol. 1 No. 1, S. 10.

nationen zentrale Lage. Ueberdies werden private, ausserhalb des nationalen Verteilernetzes liegende Linien, die frei von gestörten Verbindungen und Risiken lokaler Einmischung sind, die Attraktivität erhöhen. Dabei kommt einer Satellitenverbindung grössere Bedeutung zu, als einem mit Unterbruch gefährdeten Kabel.

Die Behörden könnten dem Land neue Einkommensquellen einer gewinnträchtigen Informationsindustrie erschliessen, unter der Voraussetzung, dass zu günstigen finanziellen Bedingungen Telephonleitungen, Satellitenverbindungen und anderes technisches Gerät unterhalten werden können, und ausserdem niedrige Importzölle auf Maschinen- und Fernmeldeeinrichtungen existieren. Haupterfordernis wird aber entweder eine Gesetzgebung mit keinem oder mangelhaften Prinzipien für Datenschutz und Datensicherheit, oder eine sehr strenge, optimalsten Persönlichkeitsschutz gewährende Rechtsordnung sein.¹¹

V. Auswahl eines "data havens" ¹²

Entscheidend für die datenverarbeitende Industrie ist bei der Auswahl einer Datenoase die Frage nach der Zweckbestimmung der Daten bzw. der Datenverarbeitung:

Benötigt ein Unternehmen einen möglichst ungehinderten und freien Informationsverkehr zur Entfaltung seiner Tätigkeit und wenig Massnahmen zum Schutz der Persönlichkeit, so wird es einen Ort wählen, an dem keine rechtlichen Einschränkungen oder eine sehr freizügige Datenschutzgesetzgebung und eine liberale Rechtsordnung in Kraft ist; i.d.R. wird hier der Export und die Verbreitung von Daten dominierend sein.

11 "Data haven" i.S. einer Abweichung nach oben, vgl. vorne, S. 34.

12 Bei einer Auswahl von "data havens" sind bereits utopisch anmutende Projekte in Betracht gezogen worden: Die Anregung, Datenbanken und Kommunikationseinrichtungen mittels Space Shuttle in das Weltall zu verlegen, um bestehenden Schranken auszuweichen, ist theoretisch durchführbar; der praktischen Verwirklichung stehen immense Kosten entgegen, die durch einen speziell gebauten Compactcomputer mit hoher Zuverlässigkeit, ausreichender Energieversorgung und "remote hardware/software maintenance" usw. verursacht würden (NORMANN, Information Privacy, Vol. 1, No. 1, S. 11).

Stehen jedoch andererseits, innerhalb der verschiedenen Aspekte der freien Marktwirtschaft, Diskretion und absoluter Schutz nicht nur personen-, sondern auch sachbezogener Daten im Vordergrund, wird die Verlagerung der Daten in ein Land mit restriktivem Datenschutzgesetz attraktiv.¹³ Eine sehr eingeschränkte Datenschutzregelung alleine wird in diesem Falle noch nicht genügen, vielmehr muss Schutz und Vertraulichkeit der Daten sich im Kontext der gesamten Rechtsordnung als optimal erweisen. Dementsprechend wird der in das Land fließende Datenstrom grösser sein, als der das Land verlassende, weil die Hauptaufgabe einer solchen nationalen Datenverarbeitungsindustrie sich eher auf die Verarbeitung, Speicherung und Verwaltung dieser Daten verlagert und der Verbreitung solcher Information nur untergeordnete Bedeutung zukommt.

In diesem Zusammenhang wird ein weiterer Problemkreis sichtbar und verständlich: Es ist durchaus möglich, dass sich innerhalb des freien Wirtschaftssystems aus finanziellen Erwägungen eine Datenverarbeitungsphasen-spezifische Auswahl bei Datenoasen durchsetzt, d.h. die verschiedenen Datenverarbeitungsphasen, wie Sammeln, Erfassen, Verarbeiten, Speichern, Verteilen, werden in verschiedenen Ländern entsprechend der günstigsten Kostenlast durchgeführt, so dass die Daten dabei unter verschiedene Rechtssysteme und unterschiedliche Schutzbestimmungen fallen. (Bei Persönlichkeitsverletzungen wird es daher Schwierigkeiten geben, a posteriori zu analysieren, in welcher Datenverarbeitungsphase die Verletzung stattgefunden hat und welches Recht damit anwendbar ist.¹⁴) Die Auswirkungen eines in diverse Länder "aufgesplitteten" Datenverarbeitungsphasen-Verfahrens ist anhand eines Modellfalles ersichtlich:

Das Sammeln von Daten erfolgt normalerweise immer an dem Ort, der die Daten liefern kann bzw. für die Auswertung erheblich ist (kann aber auch aus bestehenden Datenbanken an einem andern Ort geschehen); hingegen kann das Erfassen und Einspeichern der gesammelten Daten an

13 Vgl. Schweiz als Bankenland und Finanzplatz.

14 Vgl. vorne S. 11, Anm. 12.

einem andern Ort erfolgen, z.B. in einem Niedriglohnland der dritten Welt, das seinerseits nicht die gleiche Stufe technologischen know-hows haben muss, wie das die Daten verarbeitende Land; danach würden diese Daten wiederum in ein Industrieland mit hochentwickelter Datenverarbeitungstechnologie zur intelligenten Verarbeitung und Auswertung transferiert und letzten Endes entsprechend der Datennatur und den Erfordernissen weiterer Zugriffe entweder in einem Land mit extensivem Schutz oder an einem Ort ohne einschränkende Bestimmungen gespeichert, der eine Weiterverbreitung problemlos ermöglicht.

VI. Vermeidung von "data havens"

Um der Entstehung von "data havens" entgegenzuwirken, müssten auf internationaler Ebene einige Punkte überprüft werden:

1. Internationaler Fernmeldevertrag ¹⁵

Die Telekommunikation jedes Staates, somit auch "potentieller data havens", beruht auf der Malaga-Torremolinos Konvention von 1973, die das uneingeschränkte Recht jedes Staates anerkennt, sein Fernmeldewesen selbst zu regeln.¹⁶ Auf dieser Rechtsgrundlage hat jedes souveräne Land die Möglichkeit, eine zur Schaffung von Datenoasen attraktive und konforme Regelung seiner Telekommunikation einzuführen.

Der Internationale Fernmeldevertrag regelt aber nicht expressis verbis die Uebermittlung elektronischer Daten, sondern definiert als Fernmeldeverkehr "jede Uebermittlung, jede Aussendung oder jeder Empfang von Zeichen, Signalen, Schriftzeichen, Bildern, Lauten oder Nachrichten jeder Art über Draht, Funk, optische oder andere elektromagnetische Systeme."¹⁷ Diese Begriffsbestimmung umfasst demnach auch die Uebermittlung von elektronischen Daten (z.B. über Telephonleitungen).¹⁸ Die allgemeinen Bestimmungen über den Fernmeldedienst

15 Abgeschlossen in Malaga-Torremolinos am 25. Okt. 1973; Beitritt der Schweiz am 28.4.1976.

16 Internationaler Fernmeldevertrag, AS I 1976 S. 993, Präambel.

17 A.a.O., Anlage 2, S. 1058.

18 MALLMANN, International Agreements, S. 2, N 7.

lassen erkennen, dass sie hauptsächlich für die traditionellen Kommunikationsmedien, wie z.B. Telex, Telefon etc., konzipiert sind und weniger auf die Benutzung von elektronischer Computerkommunikationstechnologie zugeschnitten sind, aber trotzdem auch teilweise für den grenzüberschreitenden Datenverkehr Bedeutung haben. Weil der grösste Teil der Bestimmungen noch aus früheren Verträgen stammt, wurde nur der Wortlaut angepasst; im Zeitpunkt der Beschlussfassung sind die Bedeutung und potentielle negative Auswirkungen der elektronischen Datenübermittlung noch nicht bekannt gewesen, so dass die ITU¹⁹ über keine Rechtsmittel verfügt, die für den Datenschutz negative Auswirkungen zu korrigieren und nur in Übereinstimmung mit andern Ländern generelle Vorkehrungen erlassen kann, um private Telegrammübermittlungen zu unterbrechen oder eine Aufhebung des internen Telekommunikationsdienstes für spezielle Korrespondenzarten zu bewirken. Die im internationalen Fernmeldevertrag für den grenzüberschreitenden Datenverkehr zutreffenden Bestimmungen gelten aber nur solange, als die Daten über die Fernmeldeleitungen gehen.²⁰

Es existieren aber keine Regeln, die Privatsphäre und Daten (auch personenbezogene) sichern und schützen. Das Abwehrdispositiv ist in dieser, die internationale Kommunikation regelnden Konvention zu schwach und zu unvollständig. Will man der Umgehung nationaler Gesetzgebung durch Entstehung von "data havens" wirksam begegnen, muss auf internationaler Ebene eine Korrektur bzw. Anpassung bzw. Ergänzung im Rahmen eines internationalen Abkommens erfolgen, die die elektronische Datenübermittlung und deren freien, ungehinderten Fluss über die nationalen Grenzen berücksichtigt und Vorkehrungen zur Verhütung von Datenoasen und zur Sicherung der persönlichen Privatsphäre gewährleisten. Ohne eine diesbezügliche Normierung kann das Bestreben nach freiem grenzüberschreitenden Informationsfluss gefährdet sein, weil sich die Nationen mit spezifischen Datenschutz-Standards durch nationale Verordnungen wie Exportboykott oder durch bilaterale Verträge zu schützen versuchen.

19 ITU: International Telecommunications Union.

20 MALLMANN, a.a.O., S. 3, N 9.

2. INTELSAT-Abkommen ²¹

Das INTELSAT-Abkommen ist die Uebereinkunft zur Gründung der Internationalen Fernmeldesatellitenorganisation, deren Zweck es ist, auf kommerzieller Basis und in nicht diskriminierender Weise öffentliche Fernmeldeverbindungen von hoher Qualität und Zuverlässigkeit in allen Bereichen der Welt zur Verfügung zu stellen. In seiner Definition des Begriffes "Fernmeldeverkehr" ist das Uebereinkommen ebenso allgemein wie der Internationale Fernmeldevertrag, so dass es auch für die via Satelliten erfolgende grenzüberschreitende Übermittlung von Daten Geltung hat.²² Auch mittels dieses Abkommens könnte den "data havens" als Sanktion nicht mit Diskriminierung begegnet werden.

3. UNESCO Deklaration zur Satellitenübertragung ²³

Die Erklärungen enthalten Grundprinzipien, die bei Satellitenübertragungen u.a. die Respektierung der Souveränität aller Staaten voraussetzen und sie dabei ohne Diskriminierung von den Vorteilen der Satellitenübermittlungen profitieren lassen; internationale, zwischenstaatliche und fachliche Zusammenarbeit soll Grundlage für die Verwendung von Satellitenübertragungen sein.

Diese Deklaration ist aber ebensowenig wie das INTELSAT-Abkommen zur Vermeidung von "data havens" geeignet, da sie rein grundsätzlicher Natur ist und nicht gezielt zur Übermittlung computerisierter Daten Stellung nimmt - bei der Verkündung dieser Grundsatzerklärung waren die mit dem internationalen Datenaustausch zusammenhängenden Fragen und deren Problematik noch nicht aktuell.

21 Uebereinkommen über die Internationale Fernmeldesatellitenorganisation "INTELSAT" vom 20.8.1971: zit. MALLMANN, a.a.O., S. 6, N 10.

22 MALLMANN, a.a.O., S. 4, N 11.

23 Declaration of binding Principles on the Use of Satellite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange, vom 15.11.1972; UNITED NATIONS, Doc. 17C / Res. 4.111, 15. November 1972.

4. Internationales Rechtsvakuum

"Data havens" sind Ausprägung eines internationalen Rechtsvakuum, das nur mit geeigneten Massnahmen durch internationale Zusammenarbeit vermieden werden kann.²⁴ Diese Zusammenarbeit kann auf verschiedenen Wegen²⁵ den Gefahren der Datenoasen entgegenwirken:

- A. Mit einer Harmonisierung²⁶ der nationalen Gesetze, Verordnungen und Verfahrensweisen zum Datenschutz und Datensicherung i.S. der Empfehlungen des Europarates²⁷ der OECD. Dabei müssen entstehende materielle und formelle Unterschiede in der Ausgestaltung entsprechend der nationalen Rechtsstruktur einen gleich intensiven Schutz nicht a priori verhindern.
- B. Eine internationale Vereinbarung mit koordinierten Massnahmen und Vorkehrungen zur Vermeidung von Datenoasen wäre noch wirksamer als Harmonisierungsbestrebungen. Sie könnte die durch einzelstaatliche Lösungen hervorgerufene Wirkung des Datenprotektionismus ausschalten und durch Kollisionsnormen, gleichwertige Rechtsdurchsetzungsverfahren und Persönlichkeitsrechte den Mitgliedstaaten untereinander effektiveren Schutz und Sicherheit vor einem Rechtsvakuum verleihen.
- C. Solange aber weder Harmonisierung noch internationales Abkommen verwirklicht sind, werden die einzelnen Nationen Lösungen auf zwischenstaatlicher und multilateraler Ebene anstreben. Diese Vorgehen stellen eine Uebergangslösung dar, die positive und negative Auswirkungen haben:
Positiv zu werten ist der Versuch, der Entstehung von "data havens" entgegenzuwirken und den Individuen auch im grenzüberschreitenden Datenverkehr Schutz und Sicherheit ihrer Daten zu gewährleisten. Negativen Einfluss wird die Vielzahl von bilateralen und multilateralen Verträgen haben, die als Uebergangslö-

24 NORMANN, Information Privacy, Vol. 1, No. 1, S. 12.

25 WITTKAEMPER, S. 60.

26 Vgl. PANTAGES/PIPE, S. 115.

27 Vgl. Resolutionen (73) 22 und (74) 29.

sung - in Ermangelung einer internationalen Gesamtkonzeption - geschlossen wurden, weil der transnationale Datenaustausch auf die zwischenstaatliche Ebene begrenzt ist und durch ein Wirrwar von Abkommen für den privaten und öffentlichen Bereich unübersichtlich, beschwerlich und auch kostenträchtig wird. Im Hinblick auf eine spätere internationale Konvention könnten bestehende zwischenstaatliche Verträge Hemmnisse bilden, weil einmal Erreichtes nur mühsam, auch zugunsten einer international integrierten Lösung, wieder abgebaut wird.

Aber auch aus zwischenstaatlichen Abkommen können Datenbarrieren resultieren, wenn plötzlich neue Umgehungswege offenkundig und dementsprechend Massnahmen getroffen werden. Bilaterale Verträge sind nur eine Verlagerung der Problematik auf eine höhere Stufe, weil ein Gesamtkonzept und eine konzertierte Aktion aller betroffenen Nationen ausbleibt.

- D. Mitberücksichtigt werden sollte auch die Entstehung von "Piraten-Datenbanken",²⁸ die sich auf den Meeren der Rechtshoheit einzelner Nationen entziehen und in einem rechtslosen Raum ihre "Informations-Piraterie" betreiben können, ohne die für die Individuen bestimmten Schutz- und Rechtsnormen zu beachten. Als Vorbild einer Schutzregelung wäre das vom Europarat initialisierte "Europäische Uebereinkommen zur Verhütung von Rundfunksendungen, die von Sendestellen ausserhalb der staatlichen Hoheitsgebiete gesendet werden" vom 22.1.1965²⁹ geeignet. Diese Uebereinkunft bestraft den unbefugten Betrieb ausserhalb nationaler Hoheitsgebiete entsprechend innerstaatlichem Recht als unerlaubte Handlung und hat sich im Zusammenspiel mit der nationalen Gesetzgebung als sehr effektiv erwiesen.

28 Vgl. PIPE: At Sea over Pirate Databanks, New Scientist, 13.1.1977 (zit. Information Privacy, Vol.1, No.1, S. 9, Anm. 1).

29 European Agreements for the Prevention of Broadcasts transmitted from Stations outside National Territories, (ETS 53-1965), in: COUNCIL OF EUROPE, European Conventions, S. 234ff.

VII. Schlussfolgerung

Es ist das Bestreben aller sich ernsthaft mit dem Datenschutz beschäftigenden Länder und internationalen Organisationen, die Entstehung von "data havens" zur Umgehung und Aushöhlung der nationalen Gesetze und Rechtsordnungen durch entsprechende Massnahmen³⁰ zu vermeiden. Doch wird es m.E. auch mit solchen Vorkehrungen unter den verschiedenen Rechtsordnungen der Nationen (mit Datenschutzgesetzen) immer materielle und formelle Unterschiede in der Verwirklichung des Persönlichkeitsschutzes geben, ebenso werden Rechtsprechung und Rechtsdurchsetzungsverfahren entsprechend den nationalen Kulturkreisen voneinander abweichen und damit Raum für kleinere Datenoasen schaffen, die weder durch Harmonisierung noch durch zwischenstaatliche Verträge noch durch eine internationale Konvention vermieden werden können. Solche "small data havens" bilden sich innerhalb der den Datenschutz regelnden Industrienationen und zeichnen sich primär dadurch aus, dass sie keine Umgehung der nationalen Gesetzgebung bezwecken und fördern, sondern eine legitime Vermeidung (nicht Umgehung) nationaler Bestimmungen und damit eine normale Folge eines freien Datenmarktes innerhalb einer liberalen Informations- und Wirtschaftsordnung darstellen, die von allen in Kauf genommen werden muss.^{31 32} Diese "small data havens" bzw. "Convention havens"

30 Z.B. Harmonisierung, internationale Konvention, zwischenstaatliche Verträge.

31 In diese Kategorie würde z.B. eine Nation mit sehr restriktiven Datenschutz-Standards fallen, die aber wegen ihrer absolute Diskretion gewährenden Rechtsordnung nicht auf eine Unterwanderung anderer Datenschutzgesetze hinausläuft, sondern dem Bedürfnis nach optimalem Schutz von Persönlichkeit und Daten entgegenkommt. (Abweichung nach oben, vgl. vorne, S. 34).

32 Eine Bildung von "small data havens" ist z.B. zwischen Oesterreich und Deutschland denkbar, dergestalt, dass juristische Personen, die Wert auf einen Schutz ihrer personenbezogenen Daten legen, den Geltungsbereich des DSG aufsuchen und dem österreichischen Gesetz den Vorzug vor dem BDSG geben, weil die juristischen Personen auch geschützt sind; der entgegengesetzte

werden sich auch unter den Signatarstaaten einer internationalen Konvention bilden, - obwohl ein unausgesprochener Grundsatz³³ einer Konvention darin besteht, Verschiebungen von Datensammlungen und Datenflüssen in andere Konventionsstaaten aufgrund unterschiedlich restriktiver Bestimmungen zu verhindern - werden aber innerhalb dieser Mitgliedstaaten keinen negativen Einfluss hinsichtlich des Persönlichkeitsrechtes haben, da der Persönlichkeitsschutz allseits effektiv (so ist zu hoffen) verwirklicht sein wird. Bei einer Uebergangslösung durch zwischenstaatliche Verträge wird m.E. der Trend zu "small data havens" unter allen vertragsschliessenden Staaten zunehmen, weil eine Gesamtlösung des Problems "data havens" aussteht.

Fall ist auch denkbar: So ist eine Bevorzugung des BDSG für all diejenigen juristischen Personen opportun, die der Geltendmachung von Einsichtsrechten anderer juristischer Personen sich entziehen und die über andere juristische Personen gespeicherte Daten nicht preisgeben möchten (dieses Beispiel verdeutlicht, dass die Ausgestaltung des Datenschutzes im öffentlichen Bereich nicht analog auf den privaten Bereich übertragen werden darf, da dieser Bereich in bestimmten Fällen eine spezifische Ausprägung erfahren muss [eben z.B. die Regelung des Einsichtsrechts bei juristischen Personen]). Das BDSG schützt keine personenbezogenen Daten juristischer Personen und gewährt ihnen damit auch keine informationellen Individual- und Kontrollrechte.

33 Eine Verletzung dieses Grundsatzes wird nicht zu vermeiden sein, da sie Ausfluss des Prinzips des freien Informationsflusses ist.

II. TEIL: GRENZUEBERSCHREITENDER DATENVERKEHR

§ 7 BEGRIFF

Unter grenzüberschreitendem Datenverkehr ist jede Art von personen- oder sachbezogener (digitalisierter oder nichtdigitalisierter) Information ¹ zu verstehen, die den Rechtsbereich eines Landes verlässt und zum Zwecke manueller oder automatischer ² Verarbeitung in den eines andern tritt. Essentiale ist somit der Wechsel eines Hoheits- und Rechtsbereiches während des gesamten Verarbeitungsprozesses, d.h. zur Durchführung eines oder mehrerer verschiedener Datenverarbeitungsvorgänge ³ im Ausland.

Die Uebertragung der Daten in den andern Rechtsbereich kann auf verschiedene Arten erfolgen, dabei sind die Daten je nach Uebermittlungsart ⁴ in einem bestimmten Status anzutreffen:

I. Traditionelle Art der Uebermittlung

Für die herkömmliche, traditionelle Art der Uebermittlung per Post, Boten etc. müssen die Daten auf einem bestimmten Medium gespeichert sein, damit sie ins Ausland gelangen können; entsprechend ihrem Zustand wird unterschieden zwischen:

-
- 1 Der Begriff Information ist hier allgemein gehalten, da jedes nationale Datenschutzgesetz die Begriffsbestimmung und den Schutzbereich selbst festsetzt (i.d.R. sind die Informationen sach- oder personenbezogene Daten [vgl. z.B. BDSG § 2 Abs. 1 oder DSG § 3 Ziff. 1]), die auch für den grenzüberschreitenden Datenverkehr Anwendung findet.
 - 2 Bedeutung hat der grenzüberschreitende Datenverkehr erst durch die automatische Datenverarbeitung erlangt, weshalb oft nur die automatische bzw. elektronische Verarbeitung in den Schutzbereich der neuen Datenschutzgesetze fällt.
 - 3 Diese Phasen umfassen alle Bereiche wie Sammeln, Erfassen, Speichern, Verarbeiten, Ausgabenaufbereitung und Verteilen etc.
 - 4 Es wird hier bloss zwischen der manuellen, herkömmlichen und der automatisierten Uebermittlung unterschieden, ohne diese weiter abzustufen.

- Rohen Daten: Dies sind Angaben, die in normaler, lesbarer oder unlesbarer, codierter Form auf Listen, Formularen, in einem Text, auf Mikrofilm etc. aufgeführt sind.
- Maschinenlesbare Daten: Die Informationen sind erst teilweise maschinell verarbeitet worden, wie z.B. Lochkarten, Lochstreifen,⁵ oder sind bereits automatisierten Verarbeitungsschritten unterzogen worden und auf Magnetplatten, Bändern, Kassetten, Disketten, Magnetkarten etc. in kryptographierter oder unverschlüsselter Form gespeichert.

II. Automatisierte Uebermittlung

Die automatisierte Uebermittlungsart erfolgt meist über eine direkte Leitung bzw. Verbindung zwischen Absender und Empfänger (point-to-point-connection), aber auch über spezielle Datennetze, Satellitenverbindungen oder ev. mittels Infrarotstrahlen,⁶ Lichtimpuls etc. Die Daten sind dabei in einem computerisierten Status innerhalb des Verarbeitungssystems und werden über diese Verbindungswege automatisiert in den andern Rechtsbereich übermittelt.

Es ist aber auch denkbar, dass die automatisierte Uebermittlung mittels Funk, Telegraph oder Telex etc. durchgeführt wird. In diesem Falle werden die Daten nicht in computerisierter Form übertragen, sondern in roher oder maschinenlesbarer (z.B. auf Lochstreifen) Form. Charakteristikum ist, dass höchstens auf einer Seite (d.h. beim Empfänger oder Absender) ein Medium der elektronischen Datenverarbeitung angeschlossen ist.^{7 8}

5 FREESE (Data Flow, S. 20) zählt die erst partiell verarbeiteten Daten, die auf Lochkarten und Lochstreifen gespeichert sind zu den rohen Informationen. M.E. müssen diese Angaben ebenfalls zur Kategorie der maschinenlesbaren Daten gezählt werden, da ein Erkennen ihres Inhaltes das Vorhandensein einer Maschine (Lochkarten-, Lochstreifenleser) erfordert.

6 Bisher war eine Uebermittlung mittels Infrarotstrahlung erst auf kurze Distanzen möglich (vgl. IBM Bulletin, Nr. 117, Januar 1980, S. 19).

7 Diese Uebermittlungart wird meistens auf Telex- oder Telegraphennetzen vollzogen und ist von den Datennetzen die computerisierte Information übertragen zu unterscheiden.

Der Begriff des grenzüberschreitenden Datenverkehrs hat sich vom nationalen Datenfluss deshalb abgehoben, weil die nationalen Datenschutzgesetze entsprechend dem Territorialprinzip nur die im eigenen Lande erfolgende Datenverarbeitung zu regeln und zu schützen vermögen.

8 Vgl. Interpol Datennetz, hinten, S. 109ff.

§ 8 ERSCHEINUNGSFORMEN DES GRENZUEBERSCHREITENDEN DATENVERKEHRS

I Datennetze¹

1. Begriffsbestimmung²

In den folgenden Ausführungen wird der Begriff Datennetz als Datenkommunikationsnetz verstanden, das zur Uebertragung digitalisierter Signale zwischen Datenverarbeitungsmedien verwendet wird und an dessen Anschlussstellen ein Computer, Terminal oder andere EDV-Geräte stehen. Das Datennetz dient ausschliesslich der Uebermittlung von computerisierter Information mittels Hard- und Software; dabei ist unerheblich, ob das Netz sich aus speziellen Leitungen (z.B. Mietleitungen) zusammensetzt oder ob dabei auch Verbindungen über Satelliten und andere Uebermittlungsträger hergestellt werden. Dieser Typ von Datennetz muss aber vom Telegraphen- oder Fernschreibernetz unterschieden werden: In diesen Netzen erfolgt die Kommunikation zwischen Fernschreibern oder ähnlichen Geräten, wobei keine Computer beteiligt sind, ausser vielleicht in der Erledigung der Verteilfunktion von Nachrichten. Die Daten werden auf diesen Netzen nicht in computerisierter Form übertragen. Telegraphische Leitungen und Netze dieser Art sind sehr zahlreich, bleiben aber innerhalb dieser Gruppierung ausser Betracht.³

2. Arten von Netzen

Unter den Kommunikationsnetzen kann man allgemein nach Trägern drei Typen unterscheiden:⁴

A. Oeffentliche Datennetze sind grundsätzlich jedem Benutzer gegen Bezahlung eines Tarifes zugänglich. In Europa unterstehen diese öffentlichen Netze im allgemeinen dem Monopol der PTT-Verwaltungen

1 Vgl. auch OCDE, Utilisation des Réseaux.

2 Vgl. JOHNSON, Online, S. 157; STEINMUELLER, DVR 8/3 1979, S. 217.

3 Ausnahme: Interpolnetz, vgl. hinten, S. 109ff.

4 JOHNSON, Online, S. 158/167.

eines jeden Landes, werden von diesen konzipiert, technisch eingeführt und unterhalten. Diese Datennetze sind entsprechend der rechtlichen Monopolhoheit der einzelnen PTT in der Ausdehnung durch die geographischen Landesgrenzen beschränkt. (Eine Ausnahme bildet Euro-net,⁵ das als europäisches Datennetz von einem Konsortium der nationalen Post- und Telegraphenorganisationen der EG-Staaten verwirklicht wurde und ein intereuropäisches Netz bildet; das nordische Datennetz⁶ ist ebenfalls überstaatlich in seiner Ausdehnung.) Der Datenverkehr über öffentliche Netze tritt vor allem aus wirtschaftlichen Gründen immer mehr in den Vordergrund; als Beispiele solcher nationaler Netze können EDS⁷ in der BRD, EPSS in England, Transpac in Frankreich, RETD in Spanien genannt werden.

Im Gegensatz zu Europa unterhalten in den USA private Gesellschaften⁸ allgemein zugängliche Datennetze und stellen sie zur Benutzung zur Verfügung. Dabei gibt es eine Eigenart der Benutzung in den USA, die als zusätzliche Gruppe⁹ unter den allgemeinen Uebermittlungsträgern beschrieben werden kann: private Dienstleistungsunternehmen stellen ein ausgebautes Kommunikationsnetz zur Verfügung und bedienen sich dabei eines allgemeinen öffentlichen Uebermittlungsträgers, um dieses unabhängige Netz aufzubauen und zusammenzustellen; zusätzlich zu diesem Kommunikationsnetz bieten diese Firmen noch gewisse Dienstleistungen an, wie z.B. Bibliotheken-Service.^{10 11}

B. Gemeinschaftliche Datennetze charakterisieren sich durch eine gemeinsame Benutzung einer Gruppe verschiedener Institutionen (bzw. einer Gemeinschaft) mit gleichgerichteten Interessen. Diese Art von Datennetzen hat sich aus der Tatsache eines fehlenden Angebotes an

5 Vgl. hinten, S. 101ff.

6 Das nordische Datennetz verbindet die skandinavischen Nationen Schweden, Dänemark, Norwegen und Finnland.

7 EDS = Elektronisches Datenwählsystem.

8 Z.B. BELL Companies, AT & T.

9 Value-added carriers.

10 Z.B. Telenet, Tymshare, Graphnet.

11 Vgl. auch CASTLE, Online, S. 30ff. und JOHNSON, Online, S. 167.

Netzen mit spezialisierten Funktionen, wie z.B. Aufzeichnung, Gültigkeitsprüfung (Validation) und Sicherheit, herausgebildet und in Europa die Fernmeldeverwaltungen veranlasst, diesen Interessengemeinschaften zu ihrer Zweckverfolgung eine beschränkte Lizenz zum Unterhalt eines Datennetzes zu erteilen. Als klassische Beispiele dieser Art gelten SWIFT¹² und SITA.¹³

C. Private Datennetze bestehen aus Miet-, Wahlleitungen oder Satellitenverbindungen und gehören privaten Gesellschaften resp. Organisationen oder werden von diesen gemietet und zu eigenen Kommunikationszwecken unterhalten. In Europa dürfen diese privaten Netze wegen des PTT-Monopols keine Daten von Drittpersonen befördern, die das Netz nicht gemietet haben oder es selbst nicht in Betrieb halten; der Gebrauch des Netzes ist somit auf den einzelnen Benutzer beschränkt.

Eine spezielle Kategorie innerhalb der privaten Datennetz-Benutzer stellen die Servicebüros und Rechenzentren (time-sharing bureaux) dar, die in gewissen Anwendungen der Beförderung von Daten Dritter sehr nahe kommen und deswegen von den PTT auch streng überwacht werden.

Die privaten Datennetze sind, analog den gemeinschaftlichen Datennetzen, in Ermangelung eines öffentlichen internationalen Datennetzes durch Einzelinitiative von Gesellschaften entstanden. Viele dieser privaten Netze, die hauptsächlich von multinationalen Firmen¹⁴ und Organisationen betrieben werden, haben ebenfalls internationale Dimensionen und sind im Rahmen der normalen PTT-Bestimmungen gewachsen und haben ihren Benutzern erhebliche Vorteile und finanzielle Einsparungen gebracht, z.B. durch höhere Uebermittlungsgeschwindigkeiten als in regulären Trägermedien.

3. Entwicklungstrends

Allgemein muss festgestellt werden, dass die Entwicklung und Inbetriebnahme nationaler Datennetze in Europa in naher Zukunft sehr

12 SWIFT, vgl. hinten, S. 64ff.

13 SITA, vgl. hinten, S. 55ff.

14 Vgl. hinten, S. 81ff.

vielfältig sein wird:¹⁵ Die Vielfalt besteht dabei in der Einführung und Erprobung neuer Uebermittlungstechnologien,¹⁶ die noch kürzere Uebertragungszeiten mit teils beschleunigter Kommunikationsübermittlung zum Datenbankrechner ermöglichen. Diese verschiedenen Technologien sind deshalb bedeutsam, weil sie im grenzüberschreitenden Datenverkehr technische und tarifliche¹⁷ Barrieren darstellen können. Der Aufbau eines einheitlichen öffentlichen Netzes, wie dem

15 Vgl. JOHNSON, Online, S. 168, Tabelle 2.

16 Grundsätzlich sind die folgenden Technologien bedeutsam:

- Circuit-switching: Dieses elektronische Datenwählsystem (EDS) wird im Bereich des öffentlichen Telefon- und Telegraphennetzes (Telex) angewandt, bei dem die Fernsprechteilnehmer über Wahlleitungen direkte Kommunikation pflegen: z.B. in der BRD.
- Message-switching ist eine Technologie zur reinen Nachrichtenvermittlung und -verteilung, ermöglicht aber im Gegensatz zum circuit-switching und packet-switching keinen direkten Sprechkontakt der Kommunizierenden und ist innerhalb des Netzbetriebes wirtschaftlicher; die message-switching Technologie wird auch als Vorläufer des packet-switching bezeichnet.
- Packet-switching: Der Vorteil der Paketvermittlungstechnik besteht darin, dass mit der paketweisen Uebermittlung von Meldungen grosse Uebermittlungsgeschwindigkeiten erzielt werden; dabei erhebliche Kosteneinsparungen möglich werden; ausserdem können technische Standardisierungshindernisse (z.B. Modeminkompatibilitäten [Europa: CCITT-Standard Modems, Nordamerika: Bell System Standard Modems]) überbrückt werden. Diese Methode macht die internationale Datenkommunikation auch für mittlere und kleinere Unternehmer und Anwender attraktiv. Die Paketvermittlungstechnologie ist z.B. im Euronet oder beim Tymnet verwirklicht (die Schweiz will für die Euronetleitungen die Paketvermittlungstechnologie verwenden); (für Tymnet vgl. RETZLAFF, OevD 11/79, S. 913).

17 Eine langsamere Uebermittlungstechnologie innerhalb eines nationalen Netzes führt zu höheren Kosten wegen längerer Dauer der Uebermittlungszeit.

18 Durch den Aufbau eines öffentlichen Datennetzes in der Form von Euronet erhielten die privaten Datennetz-Anbieter und -betreiber in der Person der PTT-Administrationen starke Konkurrenz. Die Versuche der PTT mit Hilfe anderer Tarifgestaltung für private Leitungen, die Benutzer privater Datennetze zu veranlassen, ihren Datenverkehr aus Kostengründen auf das öffentliche Datennetz zu verlegen, bewirkte bei den privaten Netzwerk-Offerten erhebliche Kritik, die dieses Verhalten den PTT-Administrationen als missbräuchliche Ausnützung ihrer Monopolstellung vorwarfen

Euronet¹⁸ oder dem nordischen Datennetz,¹⁹ ist vor allem für die Zunahme des grenzüberschreitenden Datenverkehrs auf breiter Ebene, d.h. ausserhalb des Bereiches der multinationalen Gesellschaften und internationalen Organisationen mit eigenem Datennetz bedeutsam. Der gemeinschaftliche und private Betrieb von Datennetzen wird aber weiterhin eine Schlüsselfunktion für spezielle Möglichkeiten innehalten, wobei in Europa als Transportmedium - auch für besondere Anwendungen - das öffentliche Netz gegenüber privaten Leitungen zunehmen wird.

4. Internationale Uebermittlungsmedien²⁰

Im Gegensatz zu den umfangreichen Planvorhaben im Bereich des Ausbaus nationaler Datennetze, gibt es auf internationaler Ebene noch keine verbindlichen Zusicherungen über internationale Uebermittlungsmedien. In Westeuropa wurden in den letzten Jahren erhebliche Anstrengungen zum Bau eines öffentlichen internationalen Datennetzes²¹ erbracht, zu dem schon bald alle führenden Industrienationen Europas ihre Mitgliedschaft bekannt haben und das für die Zukunft der europäischen Industrie und Forschung auch bedeutend sein wird.

Die Philosophie der zentralgesteuerten Netzwerke mit verschiedenen nationalen Netzknoten als Anschlussstellen ist aber in der sich schnell entwickelnden Elektronikbranche bereits wieder überholt: Der neueste Trend tendiert zum Aufbau nationaler Datennetze,²² die miteinander durch Kommunikations-Protokolle²³ verbunden werden kön-

(ausführliche Argumentation bei WALKER, S. 183-186). Ein neues öffentliches Datennetz mit einer guten Netzarchitektur, störungsfreiem Betrieb und fairer Preisgestaltung wird m.E. keine Schwierigkeiten haben, Kunden privater Netze zur Umstellung auf das öffentliche Netz zu bewegen.

19 Vgl. LARSSON, Online, S. 55ff.

20 JOHNSON, Online, S. 159ff.

21 Euronet-Diane.

22 Z.B. England, Spanien, Schweiz, Frankreich bauen nationale Netze auf (GB=EPSS, F=Transpac).

23 Z.B. ACT/ISIS von Tymnet oder X.25.-Protokoll: ein Kommunikations-Protokoll, das die Kompatibilität der einzelnen nationalen Netze gewährleistet und einen Datenfluss in diesen zusammengesetzten Netzen, unabhängig von der Verschiedenheit des Aufbaus, der Hardware und der Software, sicherstellt (vgl. RETZ-

nen damit, - vereinfacht gesagt - analog den nationalen Telephonnetzen, mit einem Zusammenschluss der nationalen Datennetze²⁴ die internationale Kommunikation bzw. der grenzüberschreitende Datenverkehr trotz unterschiedlicher Netztechniken ermöglicht wird.²⁵ Die Netzstruktur wird über Mietleitungen und in zunehmendem Masse auch mit Satellitenverbindungen²⁶ erstellt werden.

Nebst diesen Tendenzen im Kommunikationsbereich und Netzaufbau auf supranationaler Ebene existiert bereits eine beträchtliche Anzahl von Vermittlungsstellen²⁷ bei den Fernmeldeverwaltungen verschiedener europäischer Länder, die einen Zugriff auf US-Datenbanken und Informationsdienste ermöglichen. Die Fernmeldeverwaltungen besitzen Knotenrechner, die mit Vermittlungsknotenrechner von Internationalen Fernmeldeverwaltungen (International Record Carriers [IRC]) der USA verbunden sind und den Anschluss an die US-Inlandnetze²⁸ herstellen. Die Tarife werden zwischen den amerikanischen IRC's und den PTT-Verwaltungen vereinbart, wobei z.B. Tymnet die Benutzer der Verbindung über den in den USA stationierten IRC-Vermittlungsknoten gleich behandelt, wie wenn ein Teilnehmer in den USA eine Anfrage stellen würde.²⁹ Eine zeitunabhängige Tarifbemessung nach Anzahl der übermittelten Zeichen kann einen Zugriff auf US-Datenbanken sogar wirtschaftlicher als eine gewöhnliche Telephonverbindung machen.

LAFF, Beispiel Tymnet, OeVD 11/79, S. 913).

- 24 Vor diesem Hintergrund wird auch der die Entwicklung und Zunahme von nationalen Datennetzen verständlich; vgl. vorne, S. 51, 52, Anm. 15.
- 25 Innerhalb der skandinavischen Länder bildet das nordische Datennetz das (inter)nationale öffentliche Uebertragungsmedium; auch dieses Netzwerk lässt sich mit andern Netzen, die z.B. auf EDS-Technologie beruhen, verknüpfen.
- 26 Z.T. bestehen schon Kommunikationsverbindungen via Satelliten, vgl. hinten, S. 76.
- 27 Z.B. der Concentrator bei Radio Schweiz AG in Bern für den Zugriff auf die US-Datenbank Tymnet.
- 28 Z.B. Tymnet oder Telenet.
- 29 Vgl. RETZLAFF, OeVD 11/79, S. 913f.

II. Träger von Datennetzen

Die folgenden Beschreibungen der Datennetze und ihrer Funktionen bei verschiedenen Trägern dienen m. E. einerseits der Illustration möglicher Funktionen solcher Netze sowie deren Ausmass an grenzüberschreitendem Datenverkehr und andererseits der Vertiefung des Verständnisses für die wirtschaftliche Bedeutung von Datennetzen bzw. ihrer Zweckverwendung innerhalb der komplexen Aufgabenbereiche multinational tätiger Institutionen.

2. Im privaten Bereich

A. SITA ^{30 31 32}

a) Träger

Träger des gemeinschaftlichen Datennetzes ³³ ist die Société Internationale pour la Télécommunication Aéronautique (SITA), Brüssel, mit Hauptverwaltung in Paris. Die Genossenschaft wurde 1949 von elf Fluggesellschaften ³⁴ zum Zwecke einer kooperativen und nicht gewinnstrebigem ³⁵ Airline-Telekommunikation gegründet. Die Mitgliedschaft ist nicht auf IATA-Gesellschaften ³⁶ beschränkt und umfasst heute über 230 international bekannte Flug-, Charter- und

30 KRONEBERG, OECD-ICCP1, S. 183ff.

31 Vgl. auch OCDE, Utilisation des Réseaux, S. 203ff.

32 Nebst diesem internationalen Telekommunikationsnetz unterhalten viele Fluggesellschaften auch noch ihr eigenes Datennetz, das sogar ans SITA-Netz angeschlossen werden kann: z.B. Swissair mit RESCO-PARS (= Programmed Airline Reservation System).

33 Vgl. vorne, S. 50f.

34 Z.B. KLM, TWA, Air France, Swissair, Sabena, BOAC, BEA etc.

35 In den Statuten ist nur das kooperative Prinzip, aber kein "nichtgewinnstrebigem Grundsatz" festgehalten: er ergab sich aus der Haltung der SITA-Gründer, die aus dem Ideal der Zusammenarbeit konkludent den Grundsatz der "non profit organisation" folgerten; diese kooperativen und nichtgewinnstrebigem Grundsätze sind entsprechend im Vertrag mit den einzelnen Fluggesellschaften festgelegt (vgl. Contract Tel.1/2, Undersigned Parties, Nr. 2).

36 International Air Transport Association.

Frachtgesellschaften wie auch kleine Commuter Airlines für ein Spezialgebiet des Zivilluftverkehrs in mehr als 150 Ländern. Kennzeichnend ist eine strikte Neutralität der Gesellschaft auf politischer Ebene und eine gemeinsame Kontrolle der finanziellen Aspekte und Bedienungsprobleme, die letzten Endes die Voraussetzungen für einen störungsfreien Transfer auf Mietleitungen des öffentlichen Netzes und privaten Uebermittlungsträgern sind.

b) Aufbau und Struktur des SITA-Netzes

Die heutige Struktur des SITA Datennetzes reflektiert das stetige Wachstum des Kommunikationsnetzes entsprechend den Bedürfnissen des Weltluftverkehrs. SITA unterhält für ihre Mitglieder ein weltweites Telekommunikationsnetz, das sowohl der konventionellen Telegrammvermittlung über Fernschreiber, als auch der elektronischen Datenübertragung dient.

In der Anfangsphase bestand der Netzverkehr einzig aus Telegrammen, deren Zahl aber wegen hoher Zuwachsraten (bis zu 100% p.a.) nicht mehr mit manuellem Betrieb in den Schaltzentren des Netzes bewältigt werden konnte und durch Automation abgelöst wurde (1959). Die zu Beginn der 60er Jahre erfolgte Ausstattung der Zentrale mit Nachrichtenvermittlungscomputer gestattete nicht nur eine Kostenreduktion auf der Personalseite, sondern verminderte auch die in einem halbautomatisierten Nachrichtenvermittlungssystem unvermeidlich auftretenden Uebermittlungsverzögerungen auf einen minimalen Faktor.

Seit 1975 betreibt die SITA ein Airline Passagier Reservationssystem mit einem Zentralcomputer in Atlanta, Ga. (USA); an das SITA Netz angeschlossen sind verschiedene Reservationssysteme³⁷ von grossen Fluggesellschaften. (Zu diesen Reservationssystemen haben u.U. auch andere Airlines Zugang; es können z.T. auch Daten zwischen

37 Z.B. ALPHA III der Air France in Vilgenis; BABS der British Airways in London; JALCOM2 der Japan Airlines in Tokio; CARMEL der ELAL in Tel Aviv; NATIONAL der National Airlines in Miami; QUANTAM der QUANTAS in Sydney; SAFARI der South African Airways in Johannesburg; KRISCOM der Singapore Airlines in Singapore; RESCO-PARS der Swissair in Zürich; APOLLO der United Airlines in Chicago usw.

den Gesellschaften ausgetauscht werden.)

Dieses Wachstum widerspiegelt sich zum Teil in der heutigen Struktur des Datennetzes, das sich in folgende drei Stufen gliedern lässt:³⁸

- Neun gleichberechtigte computerisierte Hauptzentren³⁹ sind durch Mietleitungen mit hohen Datenübertragungsgeschwindigkeiten untereinander verbunden und bilden den Kern des SITA Netzes, das sog. "High Level Network".
- Das "High Level Network" kontrolliert die zweite Stufe des Netzes, das sich aus kleineren Computern, sog. "Satellite Processors" konstituiert.⁴⁰ Diese kleineren Computer sind an das "High Level Network" angeschlossen und stellen die Verbindung zu wichtigen Städten wie z.B. Athen, Zürich, Kopenhagen her und dienen als Zwischenstelle für Datenstationen und Fernschreiber.
- Die dritte Stufe des Netzes sind ca. 12'000 Niederlassungen und Büros von Fluggesellschaften in 118 Ländern mit insgesamt 16'000 Fernschreibern bzw. Datenstationen - davon ca. 4000 Terminals für 30 Sitzreservationssysteme - angeschlossen.

c) Klassierung der Daten

Die auf dem SITA Netz beförderten Daten werden in zwei Klassen eingeteilt:

- Die Klasse A umfasst den Datenverkehr, der über die Datenstationen und Computersysteme geführt und gespeichert wird. Sitzreservationssysteme erzeugen nur Meldungen des Typus A.
- Die Klasse B beinhaltet den Telegraphenverkehr, der über die Fernschreiber, manuellen und computerisierten Schaltzentren vollzogen wird.

Statistische Angaben und Schätzungen demonstrieren die allgemein zu-

38 Stand am 1.1.1980.

39 In Amsterdam, Beirut, Frankfurt, Hongkong, London, Madrid, New York, Paris und Rom.
Vgl. Netzplan und Konfiguration in: OCDE, Utilisation des Réseaux, S. 206f.

nehmende Bedeutung des computerisierten grenzüberschreitenden Datenverkehrs durch ansteigende Volumen gegenüber den konventionellen Methoden der Fernschreibertechnologie:

Jahr	<u>Telegramm-Verkehr (Klasse B)</u>	<u>Datenverkehr (Klasse A)</u>
	Meldungen pro Jahr	Meldungen pro Jahr
1950	830'000	-
1960	75'000'000	-
1970	184'000'000	unbekannt
1978	390'981'799	677'995'549
1979 1. Q.	99'752'094 ⁴¹	216'074'762 ⁴²
2. Q.	113'407'340 ⁴³	297'580'615 ⁴⁴

Schätzungen der SITA ⁴⁵

1980	491'000'000	3'649'000'000
1981	525'000'000	4'467'000'000
1982	556'000'000	5'182'000'000
1983	578'000'000	6'092'000'000
1984	596'000'000	7'053'000'000

Bei der Betrachtung dieser Angaben wird die Bedeutung und jährliche Zuwachsrate ⁴⁶ des Datenverkehrs evident. Der Verkehr der Klasse B hat im Vergleich mit der Klasse A nur eine kleine Zuwachsrate, und der Anteil des Fernschreiberverkehrs (Klasse B) am Gesamtverkehr wird während der nächsten Jahre von 26% im Jahre 1980 auf 17% im Jahre 1984 abnehmen.

⁴⁰ Am 1.1.1980 waren 46 satellite processors im Einsatz.

⁴¹ Zuwachsrate gegenüber 1. Quartal 78: 15.0%.

⁴² Zuwachsrate gegenüber 1. Quartal 78: 87.0%.

⁴³ Zuwachsrate gegenüber 2. Quartal 78: 17.1%.

⁴⁴ Zuwachsrate gegenüber 2. Quartal 78: 81.4%.

⁴⁵ SITA, Was ist das?: Estimated Traffic Volumes 1980-1984.

⁴⁶ Vgl. oben, Anm. 42, 44.

Der hohe und zunehmende Datenverkehr erfordert einen steten Ausbau des SITA Netzes, dem im Fünfjahresplan 1980 bis 84 durch die Erneuerung des bestehenden Netzes Rechnung getragen wird. Dieses neue "Advanced Network" wird in zwei Stufen ausgebaut:

1. Das Network Control System (NCS) übernimmt die Betriebs- und Netzwerksteuerung sowie Kontrollfunktionen und Gesamtüberwachung des Netzes, um eine weitere Automatisierung zu erreichen.
2. Das Data Transport System (DTN) wird Aufgaben des High Level Systems übernehmen, wie Transport und Verteilung von Datenblöcken, und befördert ausschliesslich Klasse A Verkehr.

Die erste Phase ist in Planung und soll ca. 1982 mit vorerst 9 Computersystemen in Betrieb genommen werden und strebt durch sukzessive Erweiterung einen Endausbau von 21 Systemen an.

Das Netzwerk ist dabei unter sich selbst durch Knoten verbunden, die spezielle Datenverteil- oder Zwischenstationen darstellen.

d) Uebermittlungsobjekt

Je nach Anwendungsprogramm innerhalb des Datennetzes ist die Natur der Informationen bzw. die Verhältniszahl von personen- und sachbezogenen Angaben unterschiedlich:

- aa) Die Reservationssysteme enthalten mehrheitlich personenbezogene Angaben, die sich im Zusammenhang mit Flugbuchungen und Reservationen der Passagiere notwendigerweise ergeben und in entsprechenden Dateien abgespeichert werden:⁴⁷
- als minimale Reservationsdaten sind Name, Geschlecht, Telefonnummer (evtl. Adresse) und Auftraggeber der Buchung⁴⁸ gespeichert;

47 Die Datei-spezifische Abspeicherung gewisser Daten ist für weitere Anwendungsprogramme innerhalb der Flugverkehrsabwicklung wichtig, vgl. Flugabfertigung.

48 Passagier selbst, Reisebüro oder z.B. Sekretärin.

- ferner können weitere personenbezogene Informationen vorhanden sein, die für eine spezielle Betreuung erforderlich sind: Kinder, spezielles Essen, körperliche Gebrechen, Mitführen von Tieren etc.;
- für die Erledigung zusätzlicher Dienstleistungen kann ein Reservationssystem auch Angaben über Hotelbuchungen,⁴⁹ Billett-aufträge, Reservationen usw. enthalten.

In der Gruppe der personenbezogenen Daten werden nicht nur Angaben zu natürlichen Personen, sondern auch Informationen von juristischen Personen übermittelt, die teilweise auch dem geschäftlichen Geheimbereich zuzuordnen sind. Daneben gibt es auch sachbezogene Daten, die entweder mit dem Passagier - z.B. Reise-spezifikationen: Angaben über Flugnummer, Klasse, Datum, Abflug-ort und Destination - oder mit der Fluggesellschaft und deren Beschäftigungsbereich - z.B. Flugfahrplan, Flugbelegung, Gepäck-auslastung usw. - zusammenhängen. Die Angaben werden 24 Stunden nach Abschluss des letzten Fluges vom Speicher mit direktem Zugriff gelöscht und bis zu einem Jahr für spezielle Auskünfte auf Band gespeichert.

- bb) Bei Anwendungen der Flugabfertigung werden meist die personen-bezogenen Angaben des Reservationsprogrammes mit den für diesen Bereich notwendigen Sachdaten vermischt, die in verschiedenen Dateien gespeichert werden, wie z.B.
- Datei über Angaben der Fluggesellschaft,
 - Datei der Flugzeugtypen,
 - Datei des Destinationsnetzes,
 - Flugnummer und Fahrplandatei,
 - Passagierdatei mit Reservationsangaben,
 - Flugdaten-Datei mit Informationen über Fracht, Auslastung, etc.

⁴⁹ Fluggesellschaften, die eigene Hotels besitzen führen viele Buchungen über das SITA Datennetz aus.

Die Flugdaten- und Passagierdateien sind variable Datenspeicherungen: nach durchgeführtem Flug werden die obsoleten Informationen wieder gelöscht und die Dateien für eine neue Datenspeicherung reorganisiert.

- cc) Zusätzlich gibt es noch Anwendungen, die für eine Uebermittlung via SITA Datennetz zum Teil erst geplant oder bereits schon verwirklicht sind. Der Anteil an personen- bzw. sachbezogenen Informationen dieser Anwendungen schwankt beträchtlich:

Die Anwendung METEO FORECAST zur Aufbereitung mittelfristiger Flugwetterdaten enthält nur sachbezogene Daten,⁵⁰ während hingegen das SINEF (SITA Negative File) zur Verifikation von Kreditkarten eine grosse Zahl von Daten personenbezogener Natur auf das SITA Datennetz bringen wird. Mit der Automation der Frachtabfertigung durch das CARGO SYSTEM oder der Anwendung des BAGGAGE TRACING zur schnellen Lokalisierung und Rückschaffung verlorener Gepäckstücke werden ebenfalls einige für diese Aufgabenbereiche notwendige, auf Personen bezogene Angaben mit dem SITA Netz übermittelt werden.

- dd) Nebst diesen flugreiseppezifischen Anwendungen dient das SITA Datennetz auch noch andern Benutzungsarten:

Verschiedene Fluggesellschaften übermitteln ihre Buchhaltung von Auslandstationen über das SITA Netz an den Zentralcomputer der Airline zur Konsolidierung; ebenso erfolgt auch die gesamte SITA Buchhaltung und Kostenberechnung für die Fluggesellschaften über das SITA Netz an den Zentralcomputer in Paris.

- e) Sicherung

Das Datennetz, das die SITA den Mitgliedern zur Verfügung stellt, übermittelt anwendungsspezifisch die verschiedensten Arten von Daten.

50 Ebenso wie die Ersatzteilbeschaffung bei Flugzeugpannen.

Zur Sicherung der Mitteilungen auf dem Datennetz hat sich die SITA in Art. 3.4 des Vertrages zur Vornahme aller notwendigen Massnahmen verpflichtet, die für eine Uebermittlung mit äusserster Geheimhaltung und hoher Geschwindigkeit erforderlich sind. Ebenso wird sichergestellt, dass Datennetze von Fluggesellschaften, die an das SITA Netz angeschlossen werden und den Nachrichtenverkehr anderer Gesellschaften befördern, die gleichen Massstäbe für Geheimhaltung und kurze Uebermittlungszeiten anwenden wie bei eigenen Meldungen.⁵¹

Die Fluggesellschaften mit eigenen Reservationssystemen⁵² haben untereinander keinen Zugriff auf die gespeicherten Daten, sondern können nur via SITA Netz Meldungen senden und Nachrichten erhalten.⁵³

Zusätzlich zu diesen allgemeinen Sicherungsmassnahmen existieren anwendungsspezifische⁵⁴ Datensicherungseinrichtungen, die einen von der SITA und den einzelnen Fluggesellschaften gesteuerten Datenschutz zulassen. Innerhalb der gesellschaftseigenen Datennetze normiert jede Fluggesellschaft ihre Datensicherungsmassnahmen individuell.

f) Geheimhaltung

Im Vertrag der SITA mit ihren Mitgliedern⁵⁵ wird der Geheimhaltung der Mitteilungen aller Art grosse Bedeutung beigemessen und

51 Vgl. Art. 3.5 des Contract Tel. 1/2.

52 Vgl. vorne, S. 56, Anm. 37.

53 So kann z.B. ein Fluggast in New York an einem Flugschalter der United Airlines die ihr Reservationssystem ans SITA Netz angeschlossen hat, keine Auskunft über seinen bei der Swissair Niederlassung in Singapore gebuchten Flug (von Zürich nach Frankfurt mit einer Lufthansa Maschine) erfahren, hingegen hat die Niederlassung der Swissair in New York on-line Verbindung zu ihrem Reservationssystem RESCO-PARS in Zürich und kann ihm über alle bei Swissair gebuchten Flüge (auch mit fremden Fluggesellschaften) Angaben machen.

54 Die Datensicherungs- und Schutzmassnahmen sind bei der SINEF-Anwendung zur Verifikation von Kreditkarten ganz anders gelagert und erheblich grösser, als z.B. bei der METEO FORECAST Applikation zur Aufbereitung mittelfristiger Flugwetterdaten.

55 Art. 5 des Mitgliedschaftsvertrages.

den Fluggesellschaften untereinander sogar ein gegenseitiges Ueberprüfungsrecht dieser Geheimniswahrung eingeräumt. Verstösse gegen das Kommunikationsgeheimnis werden sogar als Grund zur einseitigen Vertragskündigung durch die SITA betrachtet und im Lande des Geheimnisbruchs nach den dort herrschenden Gesetzen beurteilt.

g) Verantwortlichkeit

Art. 6 des Vertrages⁵⁶ mit den einzelnen Mitgliedern schliesst jede Haftung und Verantwortlichkeit der SITA für Schäden, die im Zusammenhang mit der Verstümmelung, dem Verlust, der fehlerhaften oder verspäteten Uebermittlung von Daten entstehen können, aus. Für alle, aus Unregelmässigkeiten der Uebermittlung entstehenden Einbussen sind alleine die betreffenden Fluggesellschaften haftbar.

h) Folgerung

Das SITA Datennetz ist ein Medium und Hilfsmittel zur Bewältigung des Flugverkehrs, das mit dem computerisierten grenzüberschreitenden Datenverkehr eine schnellere Arbeitsabwicklung⁵⁷ und bessere Dienstleistungen ermöglicht. An der Entwicklung des SITA Netzes wird ersichtlich, dass bereits vor der Computerisierung des Datennetzes und der Reservationssysteme ein automationsunterstützter⁵⁸ grenzüberschreitender Datenverkehr stattgefunden hat⁵⁹ und der heutige internationale Datenfluss in einem computerisierten Netzwerk mit schneller Informationsübertragung eine der Lebensgrundlagen des Flugverkehrs darstellt.

56 Contract, Tel. 1/2.

57 Die Antwortzeiten an Datenstationen des Netzes sind auch zwischen grossen Distanzen wie z.B. Sydney - London sehr kurz (3-10 Sekunden bei hoher Prioritätsstufe, bzw. bis zu einer Minute bei normalen Anfragen).

58 Telex.

59 Vgl. vorne, S. 1, Anm. 1.

B. SWIFT ^{60 61}

a) Träger

Träger des gemeinschaftlichen Datennetzes ist die nach belgischem Recht gegründete "Society for Worldwide Interbank Financial Telecommunication S.G." (= "SWIFT") in Brüssel.

b) Entstehungsgeschichte

In den 60er Jahren entstand mit dem Ausbau der EDV in den Banken die Idee, eine Computerverbindung mit andern Finanzinstituten herzustellen, so dass 68 Banken aus Belgien, Deutschland, England, Frankreich, Holland, Italien und den USA eine Studie in Auftrag gaben, um darin die Durchführbarkeit eines internationalen Zahlungsverkehrs und die damit zusammenhängenden Mitteilungen zwischen Teilnehmerbanken prüfen zu lassen. Diese Studie endete mit einem positiven Ergebnis und führte 1973 zur Gründung der SWIFT durch 239 Banken aus 15 Ländern. Die gewaltige Zunahme an Mitgliedern seit der Initiative zur Studie von 68 auf 239 und das nach der Gründung erfolgende Wachstum der Mitgliedszahl auf über 500 im Jahre 1977 und gegen 750 Ende 1979 reflektieren das immense Bedürfnis nach einem internationalen Datennetz. Die Zukunft wird eine weitere Ausdehnung bringen und weltweit die verschiedensten Banken und Finanzinstitute miteinander verbinden.

c) Aufbau und Struktur des Datennetzes ⁶²

Das Datennetz basiert auf drei Rechenzentren mit doppelter Systemkonfiguration, die aus Sicherheitsgründen in verschiedenen und politisch stabilen Ländern ⁶³ liegen und jedes bei Naturkatastrophen, Sabotage oder andern Störungen die Tätigkeit der ausgefallenen Computersysteme übernehmen kann. Die drei Datenverarbeitungssysteme stehen durch eine Mietleitung in ständigem Kontakt miteinander. In

60 STROEMBERG, OECD ICCP1, S. 133ff.

61 Vgl. OCDE, Utilisation des Réseaux, S. 195ff.

62 Konfiguration und Netzplan vgl. OCDE, a.a.O., S. 196ff.

63 Belgien, Holland und USA.

jedem Lande mit Mitgliedsbanken steht ein programmierbarer "Concentrator"⁶⁴ als nationale Anschlussstelle, über den sich die einzelnen Datenstationen ans Datennetz anhängen können. Das Netzwerk deckt hauptsächlich Westeuropa und Nordamerika ab, vom Rechenzentrum USA aus werden auch Bankenländer des Fernstraumes (wie Japan, Hongkong, Singapore und Australien), Süd- und Zentralamerikas bedient.

d) Zielsetzung⁶⁵

Die SWIFT bezweckt mit ihrem Datennetz die Automation der Abteilungen mit ausländischem Zahlungsverkehr und bietet dem Benutzer Kommunikationsmöglichkeiten zur Uebermittlung von internationalen Bankmitteilungen, die früher durch Post, Telex oder Telegramm übertragen wurden.⁶⁶ Bei der Auslieferungszeit ist zwischen einer normalen Uebermittlungsdauer von zehn Minuten und einer Dringlichkeitsstufe von einer Minute zu wählen, womit die Vorteile gegenüber den herkömmlichen Uebermittlungsmethoden bereits evident werden.

e) Uebermittlungsobjekt

Uebermittelt werden ausschliesslich Mitteilungen, die den internationalen Zahlungsverkehr betreffen: in standardisierter Form können alle Typen von Kunden- und Banktransaktionen, wie Bestätigung von

64 Ein "Concentrator" ist eine programmierbare Kontrolleinheit, die bei der Datenübermittlung entweder mehrere eintreffende unabhängige Folgen von Datensignalen zu einer gemeinsamen Sequenz zusammenfasst oder sie wieder aufgliedert; damit dient er als Sammelstelle einer Mehrzahl von Leitungen dezentraler Systeme/ Datenstationen und kanalisiert diese auf eine Verbindung, ohne die Daten zu verarbeiten oder sie zu verändern.

65 "Au bénéfice collectif des membres de la société, l' étude, la création, l' utilisation et l' exploitation des moyens nécessaires à la télécommunication, à la transmission et au routage de messages internationaux financiers privés, confidentiels, particuliers entre les membres de la société." (OCDE, a.a.O., S. 195).

66 Diese elektronische Uebermittlung tendiert in Richtung "electronic mail".

Fremdwährungsgeschäften, Stellungnahmen und damit verbundene Nachrichten, inkl. Warnmeldungen vorgenommen werden. Es bestehen bereits Bemühungen, andere Gebiete wie Dokumentationssammlungen und Wertschriften zu implementieren. Diese Mitteilungen enthalten personen- und sachbezogene Angaben: Die Festlegung, in welchem Ausmass es sich bei den übermittelten oder gespeicherten Daten um personenbezogene Informationen handelt, ist von der Definition des Begriffes der "personenbezogenen Daten" abhängig.⁶⁷ Die für die Erledigung eines Auftrages erforderlichen Daten, die ins Ausland übermittelt werden, beziehen sich normalerweise auf:

- Auftraggeber,
- Auftragsempfänger,
- Verwendungszweck (Angaben über die Natur des Geschäfts),
- Konto- bzw. Bankverbindung.

Die Natur dieser Daten lässt gewisse Rückschlüsse zu, wie z.B. die Existenz irgendeiner geschäftlichen oder privaten Verbindung zwischen den beteiligten Personen. Dieser Informationsaustausch ist mit seinem Inhalt vom Kunden oder der Bank veranlasst worden und dient den Interessen des Auftraggebers. Die teils sensitive Natur dieser Informationen erfordert einen Schutz der übermittelten Nachrichten, die Wahrung der Persönlichkeitsrechte und der Geschäftsgeheimnisse; aus diesen Gründen sind auch die verschiedenen Datenschutz- und Sicherungsmassnahmen verständlich und notwendig.

Charakteristisch ist, dass als Auftraggeber im internationalen Bankgeschäft ganz allgemein die juristischen Personen auf der wertmässigen Seite⁶⁸ dominieren, während die natürlichen Personen mengenmässig als Auftraggeber im Zahlungsverkehr überwiegen.⁶⁹

67 STROEMBERG, a.a.O., S. 136.

68 Ein weiterer Grund, aus dem ersichtlich ist, dass die Daten juristischer Personen in einer internationalen Konvention oder nationalen Regelung des grenzüberschreitenden Datenverkehrs nicht ungeschützt bleiben dürfen (vgl. hinten, § 13, S. 337ff.).

69 NOWAK, OECD-ICCP1, S. 125.

f) Speicherung der Mitteilungen

Damit die übermittelten Meldungen wieder aufgefunden werden können, sind sie auf Plattenspeichern festgehalten und sind so innerhalb weniger Sekunden zur Abfrage verfügbar. Während zehn Tagen nach Absendung sind sie auf den Plattenspeichern sowohl der Aufgabe- als auch Empfängerstation jederzeit direkt zugriffsbereit. Meldungen, die älter als zehn Tage sind, befinden sich auf Plattenspeichern, die auf Verlangen zum Abruf der Meldung eingespielt werden und deshalb etwas mehr Zeit bis zur Verfügbarkeit benötigen. Zur Speicherung wird eine einzige Datenbank verwendet, die alle notwendigen Informationen zu Auffindungs-, statistischen und Verrechnungszwecken enthält, ebenso wie die Angaben der mit dem Transaktionsgeschäft verbundenen Personen (Absender und Adressat).

g) Sicherungsmassnahmen ⁷⁰

- Der Zugriff zum Datenverarbeitungssystem ist abgesichert: eine Datenstation kann nur mit einem Passwort und einer Folgenummer mit dem Zentralsystem in Verbindung treten. Dabei wird dem System bestätigt, mit welcher Datenstation es kommuniziert, überdies hält es die Benutzung des Computers durch die Bank, die den Anschluss herstellt, fest, und gibt der Datenstation ebenfalls den Anschluss ans SWIFT-Netz bekannt.
- Zur Sicherung der Zulässigkeit von Mitteilungen werden alle eingegebenen Meldungen vom System automatisch durchnumeriert;⁷¹ jede Meldung ohne Folgenummer wird zurückgewiesen und dem System nicht zur Speicherung übermittelt.
- Ebenso gibt es für jede Datenstation eine durchgehende Numerierung der ausgehenden,⁷² übermittelten Meldungen zur Ueberprüfung

70 Da Sicherheit und Vertraulichkeit als oberstes Gebot des internationalen Bankwesens gelten, werden die Sicherungsmassnahmen nur in ihren Grundzügen d.h. ohne Detailbeschreibung der Öffentlichkeit bekanntgegeben.

71 ISN = Input Sequence Number.

72 OSN = Output Sequence Number.

durch die Empfängerbank: fehlt einer Empfängerbank eine eingetrafene Mitteilung, ist sie verantwortlich für das Auffinden der verlorenen Nachricht und für die damit verbundenen Untersuchungen des Falles.

- Zusätzlich zur Speicherung der übermittelten Meldungen auf den Plattenspeichern, werden alle Mitteilungen für eine Periode von mindestens vier Monaten auf Bändern⁷³ gespeichert. Bei der Ueberspielung der Daten von den Plattenspeichern (Disks) auf die Bänder (Tapes) wird mit Verschlüsselungsgeräten gearbeitet, damit der Inhalt bei Diebstahl oder unautorisiertem Zugriff nicht gelesen werden kann; ausserdem ist der Zugang zu den Bändern strengstens abgesichert.
- Jede regionale Anschlussstelle verfügt über ein automatisches Wach- und Warnsystem, das unberechtigten Zugang oder technische Fehler entdeckt und diese sofort dem Rechenzentrum weiterleitet, damit die notwendigen Vorkehrungen getroffen werden, z.B. Isolierung der betreffenden regionalen Anschlussstelle.

h) Schutz der sach- und personenbezogenen Angaben bei der Uebermittlung

Das Ziel des Schutzes besteht in der Verhinderung, dass irgendwelche Personen unerlaubten Zugriff zum SWIFT-Verkehr während der Uebermittlungsdauer erhalten. Das Hauptanliegen der Sicherung und Geheimhaltung aller Meldungen während der Uebertragung wurde in der Weise verwirklicht, dass der Verkehr im Uebermittlungsnetz durch Verschlüsselungsgeräte für jeden Unberechtigten unverständlich ist und jeder von aussen, irgendwo in eine Nachricht eingefügte Zusatz die ganze Mitteilung unbrauchbar macht. Die Uebertragung im Netz erfolgt, ohne dass ein SWIFT-Angestellter Kenntnis vom Inhalt der Nachricht erlangt. In Fällen, wo Nachrichtentext von SWIFT-Personal gelesen

⁷³ Bänder dienen der langfristigen Speicherung von Daten, ermöglichen aber keinen direkten Zugriff, sondern erfordern einen sequentiellen Ablauf des Tapes und dementsprechend längere Antwortzeiten.

werden muss (z.B. off-line Suche von Meldungen), ist der Zugang zur Nachricht erst nach schriftlicher Einwilligung der Sender- oder Empfängerbank möglich. Der Eingriff selbst erfolgt unter Aufsicht eines Kontrollinspektors.

i) Verantwortlichkeit ⁷⁴

Die Verantwortlichkeit ist zwischen SWIFT und seinen Mitgliederbanken aufgeteilt und getrennt in SWIFT, Sender- und Empfängerbank:

- Die Senderbank ist grundsätzlich für alle Schäden aus verspäteter Zahlung verantwortlich, die infolge Unsorgfalt oder Fahrlässigkeit des Absenders verursacht wurden: ⁷⁵ z.B. wenn der Empfang einer Nachricht vom SWIFT nicht bestätigt wird und der Sender eine zweite, als Wiederholung markierte Eingabe unterlässt; oder eine Transaktion, für die eine SWIFT-Standardform vorgeschrieben ist, in einem andern Format gesandt wird, usw.
- Die Empfängerbank ist für alle Schäden verantwortlich, die infolge verspäteter Zahlung entstehen, wenn der Grund in einer bei der Empfängerbank liegenden Unsorgfalt oder Versagen besteht, ⁷⁶ z.B. wenn Systemmitteilungen nicht sofort beachtet werden oder keine entsprechende Überprüfung der (Zahl der) eingetroffenen Mitteilungen (anhand der OSN) stattfindet.

Für eingetroffene Mitteilungen, die unauffindbar oder verlorengegangen sind, ist die betreffende Empfängerbank sowohl für den dadurch verursachten Schaden als auch für die aus der Untersuchung entstehenden Kosten haftbar.

74 Die Erfahrungen seit 1977 zeigten, dass Ergänzungen und Nachträge der SWIFT-Datennetz-Benutzungs-Bestimmungen (User Handbook) notwendig wurden; eine Arbeitsgruppe überprüfte die Vorschriften und nahm die Anpassungen und Neuerungen vor, die im Board Paper 185 (SWIFT, Special Newsletter, April 1979) seit dem 1.7.79 in Kraft sind.

75 Vgl. Punkt 4 des Board Paper 185.

76 Vgl. Punkt 5 des Board Paper 185.

- SWIFT ist für alle Uebermittlungsmedien zwischen den nationalen Anschlussstellen (Concentrators) und den Rechenzentren, einschliesslich deren störungsfreiem Betrieb,⁷⁷ verantwortlich (ausser bei Störungen die durch höhere Gewalt oder technische Materialfehler verursacht werden), so z.B. bei Systemfehlern oder Irrtum des Personals oder wenn der Empfang einer Nachricht dem Sender zwar bestätigt, die Nachricht aber nicht auf der Liste der nicht-übermittelten Meldungen aufgeführt ist.
- Seit dem Beginn des Rechnungsjahres 1979 (1.7.79) führt SWIFT einen Posten für zufällige Zinsverluste und Schäden⁷⁸ von 20 Millionen BF im jährlichen Budget, der für die von SWIFT verursachten Schäden zur Verfügung stehen soll. SWIFT erstattet den Mitgliederbanken bei jedem Schadenfall den Betrag, der 100'000 BF übersteigt, zurück. Sollten die Ansprüche für ein Rechnungsjahr den Betrag von 20 Millionen BF übersteigen, werden die Rückerstattungen nur proportional der Gesamtsumme der Forderungen in Anteilen ausbezahlt bzw. gutgeschrieben. Bei einer ungerechtfertigten Forderung eines Klägers gegen SWIFT werden diesem 30'000 BF als Kosten berechnet.

k) Zulässigkeitsvoraussetzungen für Mitgliedschaft beim SWIFT-Datennetz

Für eine Mitgliedschaft kommen nur vertrauenswürdige⁷⁹ Finanzinstitute in Frage: für eine Aufnahme als Mitglied bedarf es erstens einer der Ueberprüfung des Gesuches und des Gesuchstellers, der gegebenenfalls eine Gutheissung zur Aufnahme durch den SWIFT-Verwaltungsrat nachfolgt, und zweitens auch der Zustimmung einer Mehrheit der Mitgliederbanken.

Die Ausdehnung des SWIFT-Netzes auf neue Länder beruht auf einer

77 Vgl. Punkt 6 des Board Paper 185.

78 Vgl. Punkt 7 des Board Paper 185.

79 Die Vertrauenswürdigkeit wird von den SWIFT-Mitgliedern des entsprechenden Landes bestätigt.

wirtschaftlichen Evaluation des potentiellen Datenverkehrs in diesem Staate, die sowohl von einheimischen Finanzinstituten als auch durch ausländische Mitglieder von SWIFT, die in diesem Lande arbeiten, erstellt wird.

1) Statistische Angaben

Unter den gegen 750 zählenden Mitgliedern des SWIFT hatten am 18.10.1979 über 50 Finanzinstitute ihren Sitz in der Schweiz. Diese Zahl ergibt im Vergleich mit anderen europäischen Staaten einen der höchsten Faktoren in Relation zur Einwohnerzahl und widerspiegelt die Bedeutung des internationalen Datenaustausches für einen wichtigen Zweig der schweizerischen Wirtschaft.

Aus der Statistik des Gesamtvolumens der Schweiz aus dem Jahre 1979 ist ersichtlich, dass die Anzahl der bei Mitgliederbanken eintreffenden Meldungen ⁸⁰ gegenüber den das Land verlassenden Nachrichten ⁸¹ um 10% - 15% überwiegt. Die Totalzahl, ungefähr 5.5 Millionen Meldungen im Jahr 1979, reflektiert den Umfang des grenzüberschreitenden Datenverkehrs allein in diesem einen Datennetz. Der Verkehr wird auch hier während der nächsten Jahre stetig zunehmen. Solche Zahlen erhärten die Forderung auf eine angemessene Beachtung der Regelung des grenzüberschreitenden Datenverkehrs in einem nationalen Datenschutzgesetz wie in einer internationalen Konvention, die den Verkehr in den bestehenden Datennetzen nicht mit restriktiven Bestimmungen lähmen sollten.

m) Folgerung

Wenn man die Zahl der angeschlossenen Mitgliederbanken und den grossen Umfang der von Privaten und Unternehmen getätigten internationalen Bankgeschäfte in Betracht zieht, ist es für den Laien verwun-

80 Gesamtvolumen der Schweiz der mit SWIFT eintreffenden Meldungen im Jahre 1979: ca. 3'100'000 (Bankinformation).

81 Gesamtvolumen der Schweiz der über SWIFT ausgehenden Meldungen im Jahre 1979: ca. 2'400'000 (Bankinformation).

derlich, dass bisher keine Pannen, Unregelmässigkeiten oder Vertrauensverletzungen dieses internationalen Datenaustausches offenkundig geworden sind - die Gründe können einerseits in einer hervorragenden Datensicherung liegen, die jeden unberechtigten Eingriff sofort erkennt und Schäden verhindert, andererseits kann ein gut strukturiertes und funktionierendes Verantwortlichkeitssystem jede Unregelmässigkeit dadurch abfangen, dass dem Betroffenen zumindest kein finanzieller Schaden entsteht. Obwohl die Datenschutzmassnahmen, die z.T. aus der nationalen Bankengesetzgebung resultieren (z.B. Bankgeheimnis), und Datensicherungsmaßnahmen bis heute ihre Wirksamkeit gegenüber möglichen Verletzungen bewiesen haben, können potentielle Verletzungen der Persönlichkeitssphäre nicht ausgeschlossen werden.

Bei all diesen Ueberlegungen ist jedoch zu bedenken, dass das SWIFT-Datennetz lediglich ein neues Medium ist und die vorhergehenden traditionellen Mittel ersetzt, indem es eine bessere Arbeitsabwicklung und Sicherung der gleichen Dienstleistungen ermöglicht. Die Unzulänglichkeiten des Post- und Telexwesens haben zu neuen Kommunikationsmethoden geführt, bei denen die Banken Komponenten ihrer bestehenden Datenverarbeitungsanlagen nebst der Erledigung hauseigener Projekte und Anwendungen auch noch zur Kommunikation mit dem SWIFT-Netz einsetzen. Das SWIFT-Netz ist ein reines Uebermittlungsnetz; im Vergleich mit andern Datennetzen (z.B. Euronet,⁸² IBM⁸³) findet innerhalb von SWIFT kein Datenbankaufbau und -nachführung, sondern nur eine Speicherung der übermittelten Nachrichten statt. Mit SWIFT bieten die Finanzinstitute keine neue Dienstleistung an, SWIFT ist nur ein anderes Uebertragungsmittel in Form des automationsunterstützten grenzüberschreitenden Informationsverkehrs, das sich in der Praxis hervorragend bewährt.⁸⁴

82 Vgl. hinten, S. 101ff.

83 Vgl. nachfolgend, S. 73ff.

84 READ, OECD ICCP1, S. 141.

C. Multinationale Gesellschaften: z.B. IBM

Multinationale Gesellschaften verfügen oft über ein eigenes Datennetz,⁸⁵ das den gesellschaftsinternen Informationsfluss zwischen den nationalen Stellen⁸⁶ einerseits und einer Zentrale⁸⁷ andererseits bewältigt.

Die heutigen Netzwerke sind in der Regel private Datennetze, die aus Miet-, Wahlleitungen oder Satellitenverbindungen bestehen und fast ausschliesslich Daten zwischen den eigenen Gesellschaften bzw. übergeordneter Muttergesellschaft und den ihr unterstellten Tochtergesellschaften austauschen.

Als rein exemplifikatives, m.E. für den grenzüberschreitenden Datenverkehr aber sehr repräsentatives Beispiel, soll an dieser Stelle das Datennetz (d.h. die verschiedenen Datennetze)⁸⁸ der IBM⁸⁹ eine allgemeine, weniger technisch orientierte Beschreibung erfahren.

a) Die Idee der Netzwerke bzw. die Zielsetzung des "networking"

Innerhalb aller IBM Niederlassungen sind verschiedene Datenverarbeitungsanwendungen, d.h. Computerprogramme auf einer Vielzahl von Datenverarbeitungssystemen in Funktion. Ein grosser Teil der Anwendungsprogramme haben nationalen Charakter⁹⁰ und werden selbständig in einem der vielen nationalen IBM Rechenzentren über die privaten nationalen IBM Datennetze betrieben. Neben den nationalen Anwendungen existieren aber auch noch internationale Applikationen,⁹¹ weil eine Verbreitung dieser Programme mit den dazugehörigen Datenbanken auf nationaler Ebene nicht wirtschaftlich⁹² und von der

85 Als bereits bekanntes Beispiel kann hier wiederum auf die Firma SIEMENS verwiesen werden: vgl. vorne, S. 12, Anm. 18.

86 Nationale Niederlassungen.

87 Z.B. Hauptverwaltungen, Hauptzentralen, Hauptquartier.

88 Vgl. folgenden Abschnitt b), S. 74.

89 International Business Machines Corporation.

90 Z.B. Programm für Gehalt- und Salärabrechnung.

91 Anwendungsprogramme.

92 Z.B. Aufbau und Unterhalt kostspieliger Informationsdatenbanken.

Funktionsbestimmung⁹³ her nicht zweckmässig wäre; diese internationalen Anwendungen werden in speziellen Rechenzentren auf sog. Applikationscomputern⁹⁴ unterhalten, nachgeführt und verwaltet.

Die Idee des "networking" besteht nun darin, den einzelnen Datenstationen der verschiedenen nationalen IBM Stätten diese Anwendungen über nationale und internationale Netzwerke zugänglich zu machen, d.h. im Prinzip soll man weltweit von jedem Terminal aus zu jeder Applikation (national oder international) in jedem Rechenzentrum Zugriff haben können, damit der Benutzer bei seiner Arbeit mit dem Netzwerk durch die Optimierung der Gesamthardware (Linien, Terminals, Netzwerksteuerung) eine grössere Effizienz erreicht.

Von diesem Konzept ausgehend, hat die IBM entsprechend ihren Bedürfnissen und Aufgabenbereichen mehrere private Datennetze aufgebaut, die in verschiedenen Bereichen unterschiedliche Funktionen erfüllen.

b) Übersicht der verschiedenen Netze

Bereichs- und benutzerspezifisch kann zwischen folgenden Netzarten unterschieden werden:

aa) Innergesellschaftliche Netze

Die grösste Netzinfrastruktur bilden die innergesellschaftlichen Netze, die ausschliesslich dem Datenverkehr und der Datenverarbeitung innerhalb der Firma dienen. Unter diesen Netzen sind, orientiert nach Benutzergruppen, Anforderungen und Einsatzgebieten, zwei Grundtypen auseinanderzuhalten.

aaa) Netze zur Verkaufsunterstützung und Geschäftsführung

Diese Netze sind kommerzieller Natur und haben eine von der Gesellschaftsstruktur unabhängige Gliederung; sie weisen aber mit ihr

93 Z.B. Programme zur Konsolidierung von Daten aus verschiedenen Ländern.

94 Computersystem, das speziell zum Betrieb einer Applikation und Unterhalt der dazugehörigen Datenbank dient.

eine gewisse Affinität auf, so dass letztere kurz dargestellt werden soll:

Die IBM besteht aus einer Muttergesellschaft, die sich aufgliedert in zwei Führungsgesellschaften,⁹⁵ die ihrerseits die geographischen Räume mit den untergeordneten nationalen Tochtergesellschaften global abdecken:

- IBM World Trade Europe/Middle East/Africa Corp. (E/ME/A),
- IBM World Trade Americas/Far East Corporation (A/FE).

Parallel zu dieser Gliederung gibt es zwei kommerzielle Netzwerke⁹⁶ mit internationalen Verbindungen, an die die einzelnen nationalen Netzwerke der verschiedenen Niederlassungen mit Terminals angeschlossen werden können. Ueber diese internationalen Leitungen hat das autorisierte Personal einerseits Zugang zu den internationalen Applikationen, andererseits kann es über diese Verbindungen auch in Kontakt mit nationalen Anwendungen anderer Länder treten: Datenträger sind die beiden Netzwerke. Diese Marketing-Netze können auch als Terminalnetze⁹⁷ bezeichnet werden, da der Zugriff des Benutzers auf die verschiedenen Applikationen interaktiv,⁹⁸ d.h. im Dialog erfolgt.

11) IBM E/ME/A Network

Dieses Netz wird auch "RESPOND-Uithoorn International Network" oder "SWITCH" bzw. "RESPOND" genannt und verbindet hauptsächlich die

95 Diese haben nur finanzielle Bedeutung, aber keinen direkten Einfluss auf die Ausgestaltung der Netzwerke.

96 Die beiden Netzwerke sind in ihren internationalen Anwendungen praktisch identisch, so dass ich mich auf eine Beschreibung des europäischen Netzes beschränken kann (vgl. hinten, S. 85ff.).

97 Als Benutzer nimmt man mit dem am Datennetz angeschlossenen nationalen Datenverarbeitungssystem Kontakt auf und wird von diesem mit Hilfe von Software über verschiedene Computer mit dem Applikationssystem verbunden: als Benutzer hat man dabei den Eindruck, als ob man mit dem Applikationscomputer direkt kommunizieren würde.

98 Die interaktive Betriebsart oder Dialogbetriebsart erlaubt bei der Abwicklung einer Aufgabe einen Wechsel zwischen dem Stellen von Teilaufgaben und den darauf stattfindenden Antworten.

westeuropäischen Staaten,⁹⁹ sowie einige Länder des Nahen Ostens¹⁰⁰ und Afrikas.¹⁰¹ Das SWITCH Netz besitzt zwei Netzwerkschaltzentren (switching centers)¹⁰² in Cosham¹⁰³ (UK) und Uithoorn (NL), die die von den nationalen Datennetzen bzw. Rechenzentren kommenden Daten empfangen und sie entweder an den die internationale Applikation führenden Computer oder an das Datenverarbeitungssystem weiterleiten, auf dem das entsprechende nationale Programm läuft. Die verschiedenen Applikationscomputer der internationalen Anwendungen befinden sich ebenfalls aufgeteilt in den Rechenzentren von Cosham und Uithoorn.

Die beiden Netzwerkzentren dienen aber nicht nur als Verbindungsstelle für die dem europäischen Datennetz angeschlossenen Nationen, sondern auch für das amerikanische Netzwerk.¹⁰⁴ Die Uebermittlung der für USA bestimmten Daten erfolgt von einem der beiden switching centers entweder über eine gemietete Atlantikleitung oder über eine Satellitenverbindung. In reziproker Weise dienen RESPOND und Uithoorn als Verbindungsstelle für die aus dem amerikanischen oder fernöstlichen Raum stammenden Daten, die an einen europäischen internationalen oder nationalen Applikationscomputer adressiert sind.

Insgesamt verfügt das IBM E/ME/A Netzwerk über zwei internationale Applikationszentren mit dazugehörigen switching centers und ca.

99 Belgien, Dänemark, Bundesrepublik Deutschland, England, Finnland (über Schweden), Frankreich, Griechenland, Holland, Italien, Irland, Norwegen (über Dänemark), Oesterreich, Portugal, Schweden, Schweiz, Spanien.

100 Israel, Saudi-Arabien, (Iran, Libanon).

101 Südafrika, (Lagos).

102 Im switching center übernimmt ein sog. Front-End Computer die Aufgaben des Empfanges, Vermittlung, Absendens und Weiterleitens von Daten. Er bewältigt auch die Funktion eines Konzentrators, der die auf einer Leitung gebündelten Daten empfängt, aufgliedert und sie an die Applikationscomputer weiterleitet, bzw. deren Antworten wieder auf eine Leitung bündelt und sie an den nationalen Auftraggeber zurücksendet, respektive an eine neue Adresse übermittelt.

103 Das Rechenzentrum von Cosham in England wird auch RESPOND genannt.

104 Vgl. nachfolgend, S. 77f.

20 nationalen Applikationszentren¹⁰⁵ mit den dazugehörigen Konzentratoren. An das Netz waren am 1.1.1980 ca. 10'000 Datenstationen angeschlossen. Für die nächsten Jahre ist ein Ausbau des Netzes, vor allem durch vermehrte Terminalanschlüsse, geplant, die zum einen Teil durch das Wachstum der Textverarbeitung und deren Integration in der Datenverarbeitung und zum andern im Ausbau der Informationsmöglichkeiten begründet sind. Als ungefähre Planungsdaten schätzt man auf Ende 1981 den Anschluss von insgesamt 15'000 Datenstationen, während bis Ende 1984 ca. 30'000 Terminals über das europäische Netz kommunizieren sollen.

22) Corporate Consolidated Data Network (CCDN)

Dieses Datennetz ist das amerikanische Gegenstück zum SWITCH. Die grundlegende Differenz liegt darin, dass dieses Netzwerk ein nationales, rein inneramerikanisches¹⁰⁶ Datennetz ist, über das - gleich wie beim SWITCH - nationale und, trotz der Beschränkung auf eine nationale Ausdehnung, internationale Applikationen erreicht werden können. Dieses IBM-USA-Netz besteht aus Mietleitungen und inneramerikanischen Satellitenverbindungen (bei grossen Distanzen).

Im Gegensatz zu IBM E/ME/A verfügt die IBM A/FE über kein Netz mit internationalen Verbindungen; die einzelnen Länder der amerikanischen Kontinente und der fernöstlichen Region sind für gewisse Applikationen lediglich am inneramerikanischen Datennetz über direkte internationale Leitungen bzw. Satellitenverbindungen angeschlossen.

Das CCDN hat aber nicht nur zwei, sondern vier Netzwerkzentren in:

- White Plains, N. Y.;
- Chicago, Ill.;
- Philadelphia, Pa.;
- Gaithersburg, Md.

105 Ein nationales Applikationszentrum befindet sich z.B. in Zürich und wird von der IBM Schweiz geführt.

106 Amerika i.S. von Vereinigte Staaten von Amerika.

Diese switching centers haben eine Sammel- und Schaltfunktion für verschiedene Regionen. Jeder Front-End-Computer hat Verbindung zu den 18 verschiedenen Applikationscomputern¹⁰⁷ mit den internationalen Anwendungen und ca. 60 Systemen mit nationalen Anwendungen.

Für die Verbindung zum europäischen Netz nach RESPOND/ Uithoorn und für die dem CCDN angeschlossenen Nationen der IBM A/FE Länder ist White Plains, N.Y. das zentrale switching center für alle im CCDN-Netz eintreffenden oder davon ausgehenden internationalen Verbindungen.

Grössere Nationen¹⁰⁸ der IBM A/FE haben selbständige Rechenzentren mit Computern für nationale und internationale Anwendungen, die über das nationale oder regionale¹⁰⁹ Netz benutzt werden können. Diese nationalen Rechenzentren verfügen aber alle über einen direkten Anschluss zum Netzwerkschaltzentrum in White Plains, um auch auf andere nationale oder internationale Datenbanken greifen zu können. Kleinere IBM Niederlassungen¹¹⁰ der amerikanischen Kontinente und des Fernostrumes verfügen über keine selbständigen Rechenzentren mit nationalen oder internationalen Anwendungsprogrammen; diese Länder sind direkt mit dem switching center in White Plains verbunden und benutzen die in amerikanischen Rechenzentren installierten nationalen und internationalen Applikationen.

Insgesamt waren am 1.1.1980 am CCDN ca. 10'000 Datenstationen angehängt; die Projektionen für die Zukunft sind zahlenmässig mit denen für SWITCH identisch.

107 Die Rechenzentren mit den verschiedenen Applikationscomputern sind über das ganze Land zerstreut: z.B. in Boulder, Co.; White Plains und Serling Forest, N.Y.; Bethesda, Md. usw.

108 Z.B. Kanada, Australien, Japan, Brasilien.

109 Wenn mehrere Länder in ein regionales Netz zusammengefasst werden, z.B. in Südamerika.

110 Z.B. Argentinien, Chile, Venezuela, Mexico, Hongkong u.a.

bbb) Corporate Job Network (CJN)

Das CJN ist ebenfalls ein privates Datennetz, muss aber vom SWITCH und CCDN hinsichtlich Ausdehnung, Aufbau und Anwendungsbereich getrennt betrachtet werden:

11) Ausdehnung

Das CJN ist im Gegensatz zu den beiden Terminalnetzen weltweit aufgebaut und verbindet ca. 300 Computersysteme¹¹¹ von Laboratorien und Produktionsstätten der IBM.¹¹² Die einzelnen am Netz angeschlossenen Computersysteme sind untereinander verbunden und werden als Knoten¹¹³ bezeichnet. Der Zusammenschluss der Systeme ist in Europa ein-sternförmig auf Hursley in England ausgerichtet,¹¹⁴ über das die zentrale Verbindung nach Kingston, N.Y. zu den in den USA und andern Kontinenten stehenden Computern hergestellt wird. In den USA selbst ist keine Struktur der Netzverbindungen erkennbar, ausser dass für die Verbindung zu den europäischen Laboratorien Kingston als Sammelknoten (gateway) dient.

Das physische Datennetz von CJN ist zum grössten Teil vom Terminalnetz (SWITCH-/CCDN-Netz) getrennt;¹¹⁵ es gibt aber einige wenige Leitungen, die sowohl Daten der Marketingnetze als auch des CJN befördern. Für die Zukunft ist eine vermehrte Teilung der physischen Träger auf den internationalen Linien geplant.

111 An den ca. 300 Computersystemen sind ca. 30'000 Terminalstationen angeschlossen (Stand 1.1.80).

112 Ueber Anschlüsse verfügen alle grossen Laboratorien, Forschungsstellen und Produktionsstätten der USA, Kanadas, Australiens, Japans und von acht europäischen Nationen, darunter auch die Schweiz mit einem Labor in Rüschlikon, ZH.

113 Netztechnisch muss man noch zwischen "end-nodes" und intermediate nodes" unterscheiden, dies kann aber in dieser Arbeit vernachlässigt werden.

114 Wegen grösserer Teilnehmerzahl ist ein zwei-sternartiger Netzwerkausbau mit zwei Zentren, die ebenfalls in RESPOND und Uit-hoorn angesiedelt und mit je einer Leitung nach Kingston versehen werden sollen, in Planung.

115 Das CJN ist deshalb von den andern Netzen getrennt, weil es separat konzipiert wurde und mit einem andern Teilnehmerkreis, d.h. aus der Laborumgebung gewachsen ist.

22) Topologie

Das Netzwerk ist in der Topologie anders als SWITCH und CCDN:

- SWITCH und CCDN sind Netze mit hierarchisch höher gestuften Netzwerkschaltzentren (switching centers), die die Zuordnung der Daten zu den nationalen oder internationalen Applikationscomputern vornehmen.
- Das Labornetz (CJN) besteht aus gleichwertigen Komponenten, den Knoten, die miteinander über verschiedene Pfade verbunden sind. Die Daten werden automatisch über das Netzwerk durch verschiedene Knotenpunkte an ihren Destinationscomputer gelenkt. Die Daten durchlaufen dabei sog. "transparent paths", eine Vielzahl von Computersystemen, die nur die Adressierung prüfen und die Daten weitersenden, ohne sie zu verarbeiten.¹¹⁶ Bei Störungen oder Unterbrüchen im Leitungsnetz nimmt die alle Computer verbindende "Job Networking Software"¹¹⁷ eine automatische Umleitung der Daten zum Bestimmungsort vor.

33) Anwendungsbereich

Das Corporate Job Netzwerk ist von seinem Aufbau und seinen Anwendungsmöglichkeiten für den Aufgabenkreis der Spezialisten in Labor- und Forschungszentren sowie den Produktionsstätten zugeschnitten. Das CJN ist ein "store and forward network",¹¹⁸ das in erster Linie die Verbindung zwischen Laborcomputern herstellt, die alle unter der gleichen Betriebssoftware arbeiten. Im Gegensatz zum Terminalnetzwerk für das "Marketing Personal" kann über das CJN nicht mit einem andern Computer interaktiv kommuniziert werden, sondern erlaubt den Benutzer des CJN den Austausch von Dateien und Nachrichten.

¹¹⁶ Deshalb "transparent path".

¹¹⁷ Netzwerksteuerungsprogramm.

¹¹⁸ Speicher-Datenübermittlungs-Netzwerk, d.h. es erfolgt eine abschnittsweise Datenübermittlung mit Zwischenspeicherung vor der Weitergabe.

Ueber das CJN werden hauptsächlich Datenbestände, Dateien, Auftragsverschiebungen¹¹⁹ und Meldungen an andere Computer übermittelt, um nachfolgend im Destinationssystem verarbeitet werden zu können. Diese Umlagerung von Datenverarbeitung auf andere Rechnersysteme erlaubt eine Ausnützung fremder Hardware- und Software-Kapazität, die lokal nicht verfügbar ist, und erweitert das Anwendungsspektrum der Spezialisten.

Ueber Schnittpunkte sind das Labor und Marketingnetz miteinander verbunden, so dass über Computer, die an beiden Netzwerktypen angeschlossen sind, der gegenseitige Zugang zu jedem Datennetz sichergestellt wird.¹²⁰

bb) Dienstleistungsnetz: European Personal Computing Service¹²¹

aaa) Struktur

Nebst den vorgenannten, für den gesellschaftsinternen Gebrauch aufgebauten Datennetzen, existiert in Europa seit 1978 ein Datennetz¹²² als gemeinsames Angebot der IBM Rechenzentren¹²³ der E/ME/A-Gesellschaft. In einem Rechenzentrum in Zoetermeer (Holland)

119 Job transfer, d.h. territoriale Verschiebungen von Verarbeitungsvorgängen.

120 Als Anwendungsbeschreibung kann folgendes Beispiel dienen, das gleichzeitig die Verfügbarkeit fremder Hardware-Kapazität demonstriert: ein Benutzer, der über eine Textapplikation (SCRIPT) im SWITCH auf dem Applikationscomputer in Uithoorn ein 1000 Seiten umfassendes Handbuch erstellt, möchte dieses anstatt auf seinem der Datensichtstation angeschlossenen langsamen Zeilendrucker auf einem Schnelldrucker mit hoher Schriftqualität erstellen lassen. Dafür sendet er den Datenbestand vom SWITCH ans CJN und adressiert die Daten an den Laborcomputer in Rüschlikon, wo ein Qualitätsschnelldrucker steht, lässt das Dokument dort ausdrucken und sich im Inland per interner Post zustellen; auf diese Weise macht er von fremder Hardware-Kapazität Gebrauch und erhält die Angaben schneller, als bei lokalem Ausdruck auf einem langsamen Zeilendrucker.

121 IBM Bulletin, Nr. 115, September 1979, S. 24.

122 Das Rechenzentrum der IBM Schweiz ist angeschlossen seit Mitte 1979.

123 Angeschlossene Länder am 1.1.80: UK, BRD, NL, B, F, CH; Anschluss geplant für E, skandinavische Länder (die skandinavischen Staaten sind gemeinsam an einem nordischen IBM-Rechenzen-

befindet sich sowohl die zentrale Steuerung des Netzwerkes als auch die HOST-Computer (Haupt- oder Wirtrechner), die eine zentrale Verarbeitung aller, aus den verschiedenen Ländern von Kunden oder nationalen IBM-Rechenzentren¹²⁴ übermittelten Daten erlauben.

Das Netzwerk ist aus sicherheitstechnischen Gründen von den übrigen multinationalen IBM-Netzen (CJN, SWITCH und CCDN) getrennt und weist keine Schnittstelle zu einem andern nationalen oder internationalen IBM-internen Netz auf. Es besteht somit keine Möglichkeit, vom EPCS-Netz auf ein gesellschaftsinternes Netz zu greifen und umgekehrt. Die absolute Trennung ist durch die Zweckbestimmung des Netzes für einen andern Benutzerkreis gegeben:¹²⁵ die IBM stellt dieses Datennetz ihren Kunden zur Verfügung, um international tätigen Unternehmen eine schnelle, sichere, einfache und günstige Datensammlung und -analyse auf europäischer Ebene, d.h. zentralisiert zu ermöglichen. Der Anschluss an das Datennetz ist grundsätzlich mit jedem Telefon über eine Verbindung¹²⁶ zum nationalen Konzentrador¹²⁷ möglich, der die Informationen weiter an den zentralen HOST-Computer ins Rechenzentrum Zoetermeer übermittelt.

bbb) Zielsetzung

Nebst verschiedenen Anwendungsprogrammen mit Computerkapazität zur zentralen Datenverarbeitung stehen auch Informationsdatenbanken zu Abfragezwecken zur Verfügung. Mit Hilfe dieser multinationalen

trum-Netzwerk angeschlossen, eine Verbindung dieses regionalen Rechenzentrum-Netzes mit dem EPCS (European Personal Computing Service) ist geplant.

- 124 Bulk transmission (= stapelweise Uebermittlung) vor allem bei der Uebertragung grösserer Datenmengen.
- 125 Sichtbares Resultat dieser Trennung sind die in den angeschlossenen Länder stehenden Konzentratoren: sie können nur vom Rechenzentrum in Holland aus programmiert werden; die nationale Stelle kann diese nur ein- und ausschalten.
- 126 In grösseren europäischen Ländern ist auch das nationale Netz der IBM-Rechenzentren mit dem EPCS verbunden und hilft die Telefonkosten durch Anwählen des nächstgelegenen Knotens auf ein Minimum zu reduzieren.
- 127 In der Schweiz entstehen nur die Telefonkosten für die Verbindung nach Zürich zum Konzentrador.

Infrastruktur und den entsprechenden Datenverarbeitungsprogrammen im Rechenzentrum, können die verschiedensten Probleme des kommerziellen Bereiches gelöst werden; Beispiele solcher Anwendungen sind:

- die Konsolidierung oder Auflösung von Daten (Budgets, Pläne, Monatsrapporte, usw.);
- zentrale Entwicklung und Wartung von Programmen (z.B. Investitionsrechnungsmodelle);
- zentrale Datenbanken (private Datenbanken über Absatzzahlen, öffentliche Datenbanken der OECD);
- Aufbau eines multinationalen Netzes.

Die Datenein- und -ausgabe kann innerhalb ganz Europa erfolgen und gestattet eine Europäisierung von nationalen Lösungen, Konsolidierungen, verbessert die Geschäftskontrolle, erlaubt dem Management eines multinational tätigen Unternehmens eine schnellere Reaktion auf veränderte wirtschaftliche und unternehmerische Bedingungen und ermöglicht eine Synchronisation der Geschäftsaktivitäten, um einige Vorteile zu nennen.

ccc) Datensicherungsmaßnahmen

Die Datensicherheit genießt einen hohen Stellenwert in den IBM-Rechenzentren allgemein und im besondern innerhalb des EPCS: Eine Vielzahl von Massnahmen wie Benutzeridentifikation, Passwort und individueller Schutz einzelner Datenbestände bilden das System der allgemeinen Schutzvorkehrungen. Ueberdies hat der Eigentümer des Datenbestandes die volle Kontrolle über Verbreitung und Zugang zu den Daten: ein software-mässiger Schutz gibt keinem andern als dem Dateneigentümer die Möglichkeit, den Datenbestand zu ändern,¹²⁸ weil jeder Benutzer über eine eigene Datenbibliothek verfügt.

128 Der Besitzer einer Identifikationsnummer kann einem Dritten unter einer andern Identifikationsnummer höchstens den Zugriff zu Daten, d.h. das Lesen derselben einräumen, er hat aber keine Möglichkeit dem Dritten einen verändernden Eingriff in den Datenbestand unter einer andern Identifikationsnummer zu erlauben.

Im Rechenzentrum selbst wird die Datensicherung durch tägliches Speichern der Datenbestände auf Magnetbändern unterstützt. Organisatorische Sicherungsmassnahmen, wie die schriftliche Verpflichtung jedes Rechenzentrumsangestellten zur Geheimhaltung aller im Rahmen seiner beruflichen Tätigkeit erlangten Kenntnisse, steigern die Datensicherheit; diese spezielle vertragliche Geheimhaltungspflicht für das fremde Daten verarbeitende Personal ist nicht identisch mit der allgemeinen Pflicht zur Wahrung von Geschäftsgeheimnissen, das einzuhalten ebenfalls bekräftigt wird.

Auf Wunsch und Kosten eines Kunden können zusätzlich kryptographische Geräte (hardware-mässig) für die Uebermittlung von Daten angeschlossen werden. Da das Datennetz ein geschlossenes Netz darstellt, wurde auf eine spezielle software-mässige Verschlüsselung verzichtet.

ddd) Natur der Daten

Die Anwendungen sind zur Zeit noch nicht ausgelegt für nichtformatierte Daten (d.h. Text bzw. Textverarbeitung), sondern enthalten nur Programme zur Verarbeitung formatierter Daten (d.h. Datenverarbeitung im herkömmlichen Sinn). Die Datenverarbeitung bezieht sich entsprechend den Applikationen und Kundenbedürfnissen sowohl auf sach- als auch personenbezogene Daten; die Angabe einer anteilmässigen Verhältniszahl ist nicht möglich, da die Datenarten von der IBM aus Datensicherungsgründen nicht einsehbar sind.

Alle Aktivitäten der Rechenzentrumsbenützer werden innerhalb dieses zentralisierten "timesharing-service" auf Bedarf von Fachleuten sowohl auf nationaler wie internationaler Ebene unterstützt; dadurch erhalten auch kleinere Unternehmen mit einem multinationalen Betätigungsfeld Zugang zu internationalen Datennetzen und damit zum grenzüberschreitenden Verkehr sach- und personenbezogener Daten sowie deren Verarbeitung im Ausland.

Nebst IBM betreiben aber noch eine Vielzahl von andern multinationalen Unternehmen und kleineren Gesellschaften Datennetze und offerieren einen Rechenzentrum-Service, z.B. Honeywell Bull mit dem Mark IV-Service, CDC mit dem CALL-Service etc.

c) RESPOND-Uithoorn International Network (SWITCH)

aa) Internationale Applikationen

Zum Verständnis des "networking" und der Anwendungsmöglichkeiten sollen an dieser Stelle einige der in den Rechenzentren von Cosham und Uithoorn laufenden internationalen Applikationen beschrieben werden; diese Beispiele geben einen Einblick in Erscheinungsformen des grenzüberschreitenden Datenverkehrs und vermitteln dem nicht mit der EDV vertrauten Leser eine konkrete Vorstellung über internationale Datenflüsse und die daraus resultierenden Vorteile für international tätige Unternehmen. (Die dabei aufgeführten Namen der einzelnen Programme mögen anfänglich verwirrend wirken, sind aber lediglich als Namen und nicht irgendwelche computerspezifische termini technici aufzufassen.)

aaa) HONE (Hands On Network Environment)

HONE ist der Sammelbegriff für ein verkaufsunterstützendes online System für alle Bereiche der Informationsübermittlung und produktiveren Arbeitsabwicklung, bestehend aus verschiedenen Programmen, die zum Teil Gruppen bilden (z.B. Aids)¹²⁹ aber auch als Einzelprogramm (z.B. Script)¹³⁰ zur Verfügung stehen.

11) Aids

Die Aids sind eine Gruppe von Programmen, die dem Personal der Verkaufsabteilungen (Verkäufer und Systemberater) im Dialog als direkte Hilfe und Unterstützung bei der Informationsbeschaffung für komplexe Berechnungen innerhalb ihres Tätigkeitsbereiches dienen.

- Konfiguratoren sind Programme, die dem Verkaufspersonal für die Ausarbeitung von Offerten über Systemkonfigurationen Preisblätter erstellen und beim Systemaufbau die Bestellung der Maschinen

129 Vgl. unten, Nr. 11).

130 Vgl. hinten, S. 87.

hinsichtlich systemtechnischen Abhängigkeiten überwachen. Die von einem Terminal an den Applikationscomputer übermittelten Daten sind hier rein sachbezogener Natur.

- Analysen- und Design-Aids sind Programme, mit denen Modelle von Hardware- und Software-Zusammenstellungen simuliert werden können. Mit diesen Programmen werden konkrete Kundensituationen ¹³¹ bezüglich Systemauslastung simuliert und dienen der optimierten Systemzusammenstellung. Die Simulation der Kundensituation bedingt eine Verarbeitung von sach- und eventuell auch personenbezogenen Daten.
- Financial Aids sind Programme zur Wirtschaftlichkeitsberechnung von geplanten oder installierten Computersystemen. Sie dienen der Berechnung von gebundenem Kapital, Verzinsung, Rentabilität, Produktivität einzelner Abteilungen und bezwecken ebenfalls eine optimierte Systembeschaffung. Die Berechnungen erfolgen mit Kundendaten, die vom konkreten Fall abhängig sind (z.B. Budget einer Abteilung, Personalkosten etc.).
- Sell- and Install-Aids beinhalten einerseits Hilfsprogramme im Zusammenhang mit allgemeinen Verkaufsstrategien von Hardware und Software Produkten mit IBM-technischen Angaben und andererseits Hilfsprogramme zur Installationsplanung, die sowohl personen- als auch sachbezogene Daten enthalten.

22) ERIF (European Retrieval of Information Facility)

ERIF ist ein online Datenbankensystem mit verschiedenen Informationsdatenbanken ¹³² über die Elektronikbranche und verwandte Gebiete, sowie allgemeinen Wirtschaftsinformationen. Die als Kurzbeschreibungen gespeicherten Dokumente der Informationsdatenbanken können mit Hilfe eines Textprogrammes gesucht und inhaltlich verar-

¹³¹ Die Simulationen werden aufgrund von Kundenangaben vorgenommen: Z.B. werden Anforderungen bezüglich Transaktionszahl gespeichert, und darauf berechnet das Programm mit individuellen Kundenangaben die Resultate der Modellkonfiguration.

¹³² Ca. 30 Datenbanken.

beitet werden. Als Beispiele solcher Informationsdatenbanken können aufgezählt werden:

- BOIS ist eine immer auf dem neuesten Stand befindliche Datenbank mit Kurzbeschreibungen aller publizierten IBM Dokumente.
- PLET ist eine Sammlung aller Ankündigungspublikationen von Hardware- und Software-Produkten und von Dokumenten zur Marketing Policy, den Produkteankündigungen und Produkteregeln.
- EPLC ist ein Software-Katalog sämtlicher IBM Programme und der dazugehörigen Bestellinformationen.
- LIBO ist eine Datenbank mit Kurzbeschreibungen von Büchern sowie Publikationen von Konferenzen und Symposien, die in der wissenschaftlichen Bibliothek der IBM in Boeblingen (BRD) verfügbar sind.

Die Datenbanken bestehen aus Kurzbeschreibungen von IBM-Publikationen und fremder Dokumentation, vor allem technischer Natur, und enthalten hauptsächlich sachbezogene Angaben. Dieses Datenbankensystem ist bezüglich Zweck und Aufbau vergleichbar mit dem im Euronet angebotenen Dokumentationservice DIANE.¹³³

33) APL-Programmierung

Eine Anwendung, die jedem IBM Angestellten mit Benutzungsberechtigung die APL-Programmierung für Ausbildungszwecke und für eigene Berechnungen im Zusammenhang mit dem beruflichen Tätigkeitsbereich erlaubt. Der Anteil von sach- und personenbezogenen Angaben ist vom entsprechenden Arbeitsbereich abhängig.

44) Script

Script ist ein Programm zur Texterstellung, das von allen autorisierten Personen zur Rationalisierung der Textverarbeitung benutzt werden kann. Innerhalb der Textverarbeitung wird aber nicht mit formatierten Angaben gearbeitet, sondern mit unformatierten Daten. Das bedeutet, dass die Datenmenge nicht abstrakt gegliedert, sondern im

133 Vgl. hinten, S. 101.

gesamten Kontext gestaltet gespeichert, übermittelt und verarbeitet wird. Dies hat zur Folge, dass die Information für jeden Unberechtigten viel leichter verständlich ist, weil er den Inhalt z.B. eines Briefes im Kontext rezipieren kann. Innerhalb der Textverarbeitung sind sowohl personen- als auch sachbezogene Angaben gespeichert.

55) FTS (Field Training System)

FTS ist ein Ausbildungssystem für das Marketing Personal. Das Programm enthält sachbezogene Angaben, die für die Ausbildung von Verkaufs- und Beratungspersonen notwendig sind.

66) Demo

Diese Applikation enthält Demonstrationsbeispiele von IBM Programmprodukten für Kunden; hier werden sachbezogene Angaben gespeichert und verarbeitet.

77) PROP (Proposal on-line Preparation)

Dieses Programm unterstützt ebenfalls die Verkaufsabteilungen und hilft mit vorgefertigten, juristisch überprüften Offerttexten die Erstellung von Offerten. Die Daten sind sachbezogener Natur.

Innerhalb der HONE-Applikation können Meldungen in beschränktem Umfang an verschiedene Benutzer gesandt werden. Diese Kommunikation beinhaltet naturgemäss weniger personen-, sondern mehr sachbezogene Informationen, die Mitarbeiter in den verschiedenen Ländern untereinander austauschen.

bbb) ETS2 ¹³⁴

Nebst den Kommunikationsmöglichkeiten innerhalb der HONE-Anwendung existiert ein spezieller, weltweiter "message switching service" für den internen Gebrauch, der als internes computerisiertes

134 European Telegraph System.

Telexsystem verwendet wird. Der in Cosham stehende Applikationscomputer von ETS2 übermittelt die für USA oder A/FE-Länder bestimmten Meldungen an den in White Plains stehenden Applikationscomputer ITPS¹³⁵ des CCDN (ITPS ist das Parallelprogramm zum ETS2 innerhalb des CCDN). Die Datenübermittlung der ETS2/ITPS Anwendung erfolgt über die Terminalnetze weltweit in alle angeschlossenen IBM Niederlassungen.

Im Gegensatz zu andern Anwendungen dient dieses Programm (gleich wie das SWIFT-Netz)¹³⁶ nur der Uebermittlung von Meldungen und Nachrichten und bezweckt weder Aufbau noch Verwaltung von Datenbanken; lediglich aus Sicherheitsgründen findet eine Speicherung der übermittelten Nachrichten während eines bestimmten Zeitraumes statt.

Die übermittelten Nachrichten sind je nach interner Mitteilung entweder sach- oder personenbezogener Natur; analog zum Telex werden mit dieser Anwendung individuelle Meldungen übertragen, die nicht grosse Datenmengen enthalten.¹³⁷ Für alle Uebermittlungen ist eine hardware-mässige Verschlüsselung mit kryptographischen Geräten geplant.

Da mit ETS2 der interne Fernmeldeverkehr vom öffentlichen Telexnetz auf das IBM-Datennetz verlegt worden ist, gilt es einige Vorzüge des computerisierten Telexverkehrs gegenüber dem herkömmlichen Fernmeldeverkehr aufzuzeigen:

- Grössere Produktivität durch vereinfachte und schnellere Eingabe am Bildschirm; kurze Wahlzeit beim Adressieren einer Meldung, weil der Computer immer empfangsbereit ist, auch beim Senden von Meldungen (Telex ist beim Ausdrucken oder Senden einer Meldung belegt); ein Adressverzeichnis aller intern angeschlossenen Destinationen zur online Abfrage ist immer auf dem neuesten Stand.

135 International Tele-Processing System.

136 Vgl. vorne, S. 87ff.

137 Für grosse Datenmengen vgl. IBTS, hinten, S. 93.

- Um einen Faktor 10-20 höhere Uebermittlungsgeschwindigkeit ¹³⁸.
- Grössere Sicherheit der übermittelten Nachrichten durch eine Vielzahl von Faktoren: im Gegensatz zum herkömmlichen Telex können im computerisierten Telexnetz die Daten zwischengespeichert werden, d.h. eingetroffene Meldungen werden solange gespeichert, bis sie vom Adressaten, der über ein Identifikationsprozedere und Passwort Zugang zum System erhält, abgerufen bzw. gelesen worden sind. (Im Gegensatz zum Computer muss der auf Empfang stehende Telex die Meldung sofort ausdrucken und hat keine Zwischenspeicherungsmöglichkeit, so dass die Meldung jedem, der Zugang zum Telex hat, offen lesbar und zugänglich ist.) Zur Datensicherung wird während fünf Arbeitstagen jede Meldung auf Magnetplatten zur online Abfrage zur Verfügung gehalten, danach wird sie während weiteren 25 Tagen auf Bändern gespeichert.
- Als weiterer Vorteil des computerisierten Telexnetzes erweist sich in der Praxis die Klassifizierung von Mitteilungen in "sog. "confidential messages", für deren Zugang zusätzlich noch ein bestimmtes Passwort benötigt wird, und in sog. "non confidential messages". Innerhalb einer Fachabteilung können alle Personen das Telexsystem unter einer bestimmten Benutzernummer gebrauchen, der Zugang zu vertraulichen Informationen ist aber auf einige wenige Personen beschränkt.
- Als Nachteil des Datennetzes muss erwähnt werden, dass nur eine "Einwegkommunikation", d.h. ein Senden von Mitteilungen stattfindet und im Gegensatz zum herkömmlichen Telex keine direkte Kommunikation möglich ist (in der Praxis ist aber die direkte Kommunikation selten).

Zur Illustration einer solchen elektronischen Nachrichtenübermittlung soll folgendes Beispiel in vereinfachter Weise die Durchgangphasen der verschiedenen Datennetze erläutern: Eine Meldung soll

¹³⁸ Der Telex übermittelt ca. 60 Zeichen / Sek.; das Computernetz überträgt mit 4800 / 9600 bit/Sek. (pro Zeichen werden 4-8 bit benötigt: für Zahlen 4 bits, für Buchstaben 8 bits).

von einem Absender XY der IBM Niederlassung in Genf in die IBM Niederlassung Melbourne (Australien) an den Adressaten XX gesandt werden. Die Meldung geht vom Bildschirm des Sachbearbeiter XY über das nationale schweizerische IBM Netz an den Konzentrador in Zürich, der die Meldung als ETS2-Anwendung identifiziert¹³⁹ und an das angeschlossene Computersystem weiterleitet. Der Computer in Zürich erkennt, dass ETS2 eine internationale Applikation ist und adressiert sie an das für ETS2 zuständige, zentrale Rechenzentrum in Cosham. Die Meldung geht an den Konzentrador zurück und wird von diesem auf die Mietleitung nach Cosham gelenkt. In Cosham trifft die Meldung bei einem Front-End Computer¹⁴⁰ ein, wird analysiert, als ETS2 identifiziert und darauf an den ETS2 Applikationscomputer mit der angegliederten Datenbank¹⁴¹ weitergegeben; dieser stellt fest, dass die Meldung für keinen europäischen Adressaten¹⁴² bestimmt ist, sondern über das CCDN-Netz geleitet werden soll und schickt die Meldung zurück an den Front-End Computer mit dem Vermerk, dass sie in die USA zum internationalen "switching center" in White Plains gesandt werden muss. Die Meldung trifft entweder über Satellit oder über eine Mietleitung im Front-End Computer des Vermittlungszentrums in White Plains ein und wird als ITPS Anwendung erkannt und an den ebenfalls in White Plains stehenden ITPS-Computer weitergeleitet. Das Applikationssystem identifiziert die Fernost-Adresse und schickt die Meldung an den Front-End Computer zurück, mit dem Vermerk Sydney, so dass sie über Satellit an den Konzentrador des nationalen Rechenzentrums der IBM Australien gelangt; dort wird die Meldung aus Genf im Rechenzentrums-

139 Der Inhalt der Meldung kann nicht analysiert werden, sondern nur Art der Applikation.

140 Vgl. vorne, S. 76, Anm. 102.

141 Hier findet aber kein spezieller Datenbank-Aufbau und -Unterhalt statt.

142 Wenn die Meldung für einen europäischen Adressaten bestimmt wäre, würde sie im Computer gespeichert, d.h. dem entsprechenden Adressaten ins "computerisierte Postfach" gelegt, bis er sie abrufen. (Telexmeldungen sind im ETS2 als Holschulden deklariert.)

computer für den Adressaten XX bis zu deren Abruf über die am IBM-Australien-Netz angeschlossene Datensichtstation in Melbourne gespeichert. Die Uebermittlungszeit einer solchen Meldung beträgt minimal zwei Minuten, vorausgesetzt, dass alle Systeme in Betrieb sind. Oft sind jedoch einige Computersysteme infolge Zeitverschiebung nicht aktiv; der die Daten weiterleitende Applikationscomputer in RESPOND und White Plains ist darüber informiert und nimmt in diesem Fall eine Zwischenspeicherung vor, bis die nächste Destination aktiv wird (store and forward-Prinzip).

ccc) FIS ¹⁴³

Das Field Instruction System ist ein Schulungsprogramm für die online Ausbildung des technischen Personals. Die Kurse wurden in einem speziellen Technikerzentrum der USA entwickelt und für die weltweite Uebernahme bereitgestellt. Die Dateien beinhalten sachbezogene Daten für mehr als 700 Kurse zur technischen Instruktion und Ausbildung über eine breite Palette von IBM Hardware- und Software-Produkten.

ddd) SECOM ¹⁴⁴

Diese Anwendung versorgt die Gruppe der Systemberater mit technischen Informationen über IBM Programmprodukte, spezielle IBM Produkte, installierte IBM Benutzerprogramme und systemtechnische Hilfe und Hilfsmittel. Das für die Systemberater bestimmte Kommunikationssystem ermöglicht ebenfalls eine Speicherung von geplanten, angekündigten, technischen, internen Ausbildungskursen.

Während jeder Nacht findet zwischen den europäischen und amerikanischen Applikationssystemen ein Austausch der sachbezogenen Daten statt, um die neuesten Informationen auf den Computern nachzuführen.

143 Field Instruction System.

144 System Engineering Communication System.

eee) RETAIN

Dieses Fehlermeldesystem hilft den Aussendiensttechnikern¹⁴⁵ bei diagnostischen Problemanalysen. Als weltweite Applikation sind in Europa und USA zusammen vier RETAIN-Systeme¹⁴⁶ installiert, die miteinander verbunden sind und die direkte Kommunikation zwischen den vier angegliederten Datenbanken ermöglichen. Die Systeme sind rund um die Uhr in Betrieb und werden mittels besonderer Techniken automatisch nachgetragen, wenn in der Datenbank eines Systems eine Aenderung oder ein Nachtrag erfolgt.¹⁴⁷

Auf den Datenbanken werden Bibliotheken mit allen bekannten Hardware- und Software-Fehlern von installierten IBM Produkten unterhalten und nachgeführt, damit eine schnellere Fehlerdiagnose erfolgen kann. Aufgrund einer Beschreibung des konkreten Falles werden sachbezogene und z.T. personenbezogene Angaben (z.B. Kundenbezeichnung) zum Problemfall gespeichert. Spezialisten erarbeiten Korrekturen und Umgehungslösungen, die der Fehlerbeschreibung hinzugefügt werden, so dass das Programm zur zentralen Fehlerbehebung dient.

fff) IBTS¹⁴⁸

Die internationale Uebermittlung von grossen Datenbeständen erfolgt auf weltweiter Ebene zwischen den IBM Niederlassungen mit der IBTS Software. Diese Uebertragung hat insofern eine Sonderstellung, als dafür verschiedene Netze verwendet werden:

- Die nationalen Hauptverwaltungen benutzen zur Uebermittlung grosser Datenmengen an das zentrale IBTS-Computersystem in RESPOND dank einer mehrfachen Ausnützungstechnik hauptsächlich das online Terminalnetz. Dabei wandern die IBTS Daten mit einer im Vergleich zum interaktiven Datenverkehr niedrigeren Prioritätsstufe¹⁴⁹ über das Datennetz an den zentralen Computer,

145 Customer Engineers.

146 In Cosham; Uithoorn; Boulder, Co.; Sterling Forest, N.Y.

147 Vgl. Beispiel hinten, S. 95f.

148 Integrated Bulk Data Transmission System.

149 Die niedrige Prioritätsstufe kommt in längeren Uebermittlungszeiten zum Ausdruck.

ohne die Verfügbarkeit der online Applikationen zu beeinträchtigen.

- Laboratorien und Fabrikationsstätten benutzen zur Uebertragung ihrer Datenbestände meistens eine direkte Verbindung ihres lokalen Computers zum "store and forward"-System¹⁵⁰ in Cosham.

Für die A/FE-Länder befindet sich das Transatlantik-Durchgangszentrum im CCDN-Vermittlungszentrum in White Plains und für die E/ME/A-Länder in Cosham. A/FE-Länder haben über die transatlantische Superleitung zwischen dem White Plains- und RESPOND-IBTS-Computer Zugriff zu E/ME/A-Niederlassungen und umgekehrt. In einigen Ländern existiert ein Computer als Speicher-Datenübermittlungsknoten.¹⁵¹

Diese umfangreichen Datenmengen in Form von Benutzerdaten, Handbüchern, Geschäftsdaten, Datenbanknachführungen, Konsolidierungsdaten, die in den einzelnen nationalen Rechenzentren auf Bändern oder Magnetplatten gespeichert sind, werden in das System eingelesen, welches sie automatisch über Zwischenknoten zum Destinationsort sendet. Die Uebertragungszeit ist von Umfang und Volumen, der Netzwerkroute und der Netzwerkauslastung abhängig. In der Regel müssen Uebermittlungen grosser Datenbestände zum voraus angekündigt werden, um genügend Kapazität des Uebertragungsnetzes sicherzustellen und damit auch datensicherungsmässig die Verschiebung der Datenmengen ohne Probleme abwickeln zu können.

Die übermittelten Daten können sowohl personen- als auch sachbezogenen Charakter haben; interessant ist dabei festzustellen, dass die Uebertragung der Daten immer in komprimierter Form erfolgt. Verschlüsselt¹⁵² wird nur auf Wunsch des Datenbesitzers zum Zeitpunkt des Einlesens mit einem vom Datenbesitzer spezifizierten Schlüssel. Entschlüsselt wird erst durch den Empfänger zum Zeitpunkt des Aus-

150 Speicher-Datenübermittlungssystem (vgl. vorne, S. 80, Anm. 118).

151 Store and forward node.

152 Software-mässig.

lesens mittels des vom Absender separat erhaltenen Schlüssels. Der Schlüssel wird ebenfalls in verschlüsselter Form übermittelt.

bb) Beispiele der Benutzung von Anwendungsprogrammen

Zur Illustration der Benutzung des Datennetzes und der damit angebotenen Applikationen sollen die folgenden Beispiele dienen, die gleichzeitig den grenzüberschreitenden Weg der Daten beschreiben.

aaa) Beispiel einer internationalen Applikation

Ein Techniker in Bern findet bei einem installierten IBM Computer oder Programm einen Fehler; zur Diagnostizierung des Fehlers bedient sich der Techniker einer am Terminalnetz angeschlossenen Datestation, um mittels der Applikation RETAIN¹⁵³ eine Lösung seines Problems zu suchen. Seine Anfragen werden über das schweizerische IBM Datennetz an den nationalen Konzentrador in Zürich geleitet und dort dem angeschlossenen Computersystem im Rechenzentrum übergeben, das die Daten als internationale Applikation RETAIN erkennt und sie entsprechend adressiert. Vom Computer gehen die Anfrage-Daten des Technikers an den Konzentrador zurück, der die vom System vorgenommene Adressierung liest und sie entsprechend an den Front-End Computer in Cosham oder Uithoorn übermittelt. Die Daten werden darauf dem zuständigen Applikationssystem mit der angegliederten Datenbank übertragen, das die Abfragen auswertet und hierauf die Antwort und die Lösung auf dem gleichen Weg in umgekehrter Richtung nach Bern mit einer Lösung sendet. Auf diesem Wege kann der Techniker die in der Datenbank des Applikationscomputers RETAIN aufgeführten Problembeschreibungen in einem ähnlich gelagerten Fall überprüfen und den von Spezialisten ausgearbeiteten Lösungsvorschlag zur Fehlerbehebung verwenden. Existiert auf dem Applikationscomputer keine analoge Problembeschreibung mit der entsprechenden Lösung, gibt der Techniker selbst eine Dar-

153 Vgl. vorne, eee), S. 93.

stellung des Problemfalles in die RETAIN-Datenbank ein, welche von einem Spezialisten analysiert und mit einem Lösungsvorschlag versehen wird. Sowohl die Problembeschreibung als auch neue, von einem Spezialisten erarbeitete Lösung wird in Minuten mittels eines automatischen Nachführungsprogrammes auf allen vier zentralen RETAIN-Computern des SWITCH und CCDN Netzes nachgeführt, so dass ein Techniker, der ein gleichgelagertes Problem wenig später in Tokio entdeckt und über sein nationales Netz auf den RETAIN-Computer in Boulder zugreift, die vor kurzem eingegebene Problemdarstellung zugestellt erhält und, wenn noch keine Lösung vorhanden ist, weiss, dass an einer Umgehung gearbeitet wird und diese abwartet, oder, wenn bereits Lösungsvorschläge abgespeichert wurden, diese zur Problembehebung verwendet.

bbb) Beispiel einer nationalen Applikation

In Orly (F) existiert eine nationales Programm (ORLIMS), das eine Ersatz- und Bestandteile-Organisation beinhaltet und Auskunft gibt über die Bezeichnung der gelagerten Teile, den Ort der Lagerung, ihre Anzahl, Verfügbarkeit, Kosten etc. Ein Techniker in Lugano, der Ersatzteile benötigt, kann, sofern sie im nationalen Lager nicht mehr vorhanden sind, ausfindig machen, auf welchem Wege sie am schnellsten erhältlich sind. Dazu nimmt er mit dieser nationalen Applikation in Orly Verbindung auf; seine Anfrage wird von Lugano aus über das nationale schweizerische IBM Netz an den Konzentrator in Zürich geleitet und dem Computer im Rechenzentrum übermittelt, der die Daten als französische, nationale Applikation identifiziert, adressiert und sie wieder dem Concentrator zur weiteren Uebermittlung nach Cosham zurückgibt. Im Front-End des internationalen Vermittlungszentrums von Cosham werden sie als französische, nationale Applikation identifiziert und direkt an den nationalen Konzentrator der IBM Frankreich in Paris weitergeleitet. Der Konzentrator übernimmt nun die Verteilerfunktion und vermittelt die Abfrage-Daten dem Applikationscomputer ORLIMS in Orly. Auf dem gleichen Weg werden die Antworten zurückgesandt, so dass der Techniker mit Hilfe dieses nationalen Programmes in Frankreich ausfindig machen kann, auf welchem Weg die Ersatzteile am schnellsten erhältlich sind.

cc) Datensicherung und Datenschutz

aaa) Eine Vielzahl von Datensicherungsmaßnahmen technischer und organisatorischer Natur zielt auf einen optimalen Schutz der Daten während der verschiedenen Transportphasen. Dazu gehört die Festlegung der Verantwortlichkeiten für Fernmeldenetz und Applikationen z.B. in Form von:

- Passwort, dessen Unsichtbarkeit und Generierung;
- Benutzeridentifikation;
- spezielle Bildschirmmasken für gewisse Datenstufen;
- Druckmöglichkeiten nur an gewissen Orten;
- Speicherung von Nachrichten nach Klassifikationsstufen und entsprechender Einsichtsbeschränkung.

Neben den Verantwortlichkeiten wird dem mit Netzwerk und Applikationen arbeitenden Personal eine Anzahl von Pflichten auferlegt, die der Datensicherung förderlich sind, so z.B.:

- Klassifizierung der Ein- und Ausgaben, der Daten und der Programme;
- Bezeichnung der sensitiven Programme;
- Festlegung von Kontrollelementen;
- Ueberwachung der anzuwendenden Kontrollvorschriften während Entwicklung, Ausbau und Betrieb der Uebertragungsmedien und Maschinen.

Zu den organisatorischen Vorschriften kann auch die Schaffung von Datenkategorien nach deren "Gefährlichkeit bei Missbräuchen" und eine entsprechende Klassierung der Daten gezählt werden.¹⁵⁴ So bestehen gesellschaftintern strenge Richtlinien bei der Handhabung von personenbezogenen und sachbezogenen Daten, die dem Schutzbedürfnis der Information Rechnung tragen; das Schutzbedürfnis reflektiert sich in den verschiedenen Klassifikations-Stufen der Daten, die eingeteilt sind in:

- registered IBM confidential

154 Vgl. auch PAWLIKOWSKI, Datensicherheit, S. 11.

- IBM confidential-restricted
- IBM confidential
- IBM internal use only
- not classified

Diese Abstufung hat sowohl organisatorische Auswirkungen auf den Personenkreis, dem Daten kundgegeben werden, als auch auf deren elektronische Uebermittlungsmöglichkeit in den verschiedenen Datennetzen. Im IBTS-Netz existieren andere Handhabungsvorschriften und Uebermittlungszulassungen bezüglich der verschiedenen Datenstufen als im Terminal- oder Labornetz. Die Vorschriften und Verantwortlichkeiten sind klar definiert.

Nebst diesen Richtlinien zur Datenhandhabung wird das Personal, dem vertrauliche Informationen und Unterlagen anvertraut werden, angehalten, ein oder mehrere sog. "non disclosure agreements" zu unterzeichnen, mit denen jeder Einzelne sich zur Wahrung der Vertraulichkeit der im Rahmen seiner Tätigkeit erlangten Kenntnisse gegenüber unberechtigten Mitarbeitern und Dritten verpflichtet.

bbb) Bei der Kryptographie gibt es grundsätzlich zwei Arten der Verschlüsselung, die alternativ angewandt werden und von der Klassifikationsstufe der Daten und der Art des Datennetzes abhängen:

- software-mässig wird mit Verschlüsselungsprogrammen gearbeitet: Der Schlüssel im Computerprogramm ist dabei unter allen miteinander kommunizierenden Datenverarbeitungssystemen gleich. In unregelmässigen Intervallen erfolgt eine Aenderung des Schlüssels. Im Zusammenhang mit den "Verschlüsselungsschlüsseln" existieren eine Reihe von zusätzlichen Massnahmen und Vorschriften, die das Datensicherungskonzept verstärken; so ergibt sich z.B. aus dem Gebrauch unterschiedlicher Schlüssel für die verschiedenen Datenklassen eine weitere Verfeinerung.
- hardware-mässig dienen mit Computersystemen gekoppelte Verschlüsselungsgeräte der Datensicherheit, indem sie alle durch sie übermittelten Informationen chiffrieren bzw. dechiffrieren. Für die internationalen Verbindungen ist eine hardware-mässige Verschlüsselung in stufenweisem Ausbau.

ccc) Im Rahmen des ständigen Ausbaus und der Erweiterung der Datennetze wird eine Verfeinerung und Optimierung der internen Datensicherungs- und Schutzmassnahmen angestrebt. Als Beispiel von solchen verbesserten Datenschutzvorkehrungen kann die für das Labornetz erlassene Bestimmung angeführt werden, wonach jedes am CJN angeschlossene Computersystem die Verantwortung für die Einhaltung der lokalen Rechtsvorschriften zum Schutz der Persönlichkeit und Datensicherheit trägt, so dass es u.U. erforderlich sein kann, Benützern, die grundsätzlich Zugang zu personenbezogenen Angaben haben, den vom Ausland her erfolgenden Zugriff über das Datennetz zu sperren.

d) Folgerung

Die vielfältigen Anwendungsmöglichkeiten und Vorteile der einzelnen Datennetze und deren komplexe Verflechtung untereinander, zeigen die wirtschaftliche Bedeutung ^{70a} des grenzüberschreitenden Datenverkehrs innerhalb multinational tätiger Firmen auf. Angesichts der mit verschiedenen Applikationen durchführbaren Anwendungsvarianten, allein innerhalb des skizzierten europäischen Marketing-Netzes, ist der tägliche Umfang des grenzüberschreitenden Datenverkehrs nur zu erahnen. Trotz des hohen Volumens des internationalen Datenflusses sind dank organisatorisch gut ausgebauten Datensicherungsmaßnahmen noch keine Missbräuche registriert worden: ein Beweis für den Stellenwert der Datensicherung, vor allem im grenzüberschreitenden Datenverkehr und deren Effizienz und Wirkungskraft bei einer optimalen gesellschaftsinternen Organisationsstruktur.

Die Charakterisierung des grenzüberschreitenden Datenverkehrs als "Blutkreislauf der multinationalen Gesellschaften"¹⁵⁵ ist nicht verfehlt. Dabei ist aber auch zu bedenken, dass von den multinationalen Firmen in verschiedenen Branchen, wie z.B. Elektronik oder Chemie, umfangreiche Forschungs- und Entwicklungstätigkeiten ge-

155 SERWATYNSKI, Information Privacy, Vol. 1, No. 2, S. 81.

tragen werden, die durch ihre Innovationen nicht nur dem Einzelnen, sondern der ganzen Gesellschaft nützen. Voraussetzung dafür ist allerdings eine umfassende Kooperation zwischen den einzelnen Laboratorien, die ohne internationalen Informationsverkehr, d.h. Datenaustausch, nicht gewährleistet wäre. Eine ungerechtfertigte Beschränkung des grenzüberschreitenden Datenflusses durch verschiedene Nationen könnte deshalb verhängnisvolle Folgen für die international tätigen Unternehmen, die Entwicklung und Forschung in der gesamten Wirtschaft haben und letztlich jeden Einzelnen treffen.

2. Im öffentlichen Bereich

A. EURONET - DIANE ^{156 157}

a) Aufbau und Träger

Beim Euronet-DIANE sind zwei Teile auseinanderzuhalten:

- Euronet, ist das physische Datennetz, das auf Initiative der Kommission der Europäischen Gemeinschaften als Gegenstück zu den amerikanischen Netzwerken ¹⁵⁸ konzipiert, von der EG entwickelt und von einem Konsortium der nationalen Fernmeldeverwaltungen und -organisationen (PTT)¹⁵⁹ der Mitgliedstaaten der Gemeinschaft errichtet und eingeführt wurde. Die Fernmeldeverwaltungen der EG-Mitgliedstaaten und der mit diesen Verwaltungen durch Abkommen verbundenen Staaten ¹⁶⁰ sind Träger des Datennetzes und für den Betrieb verantwortlich.¹⁶¹ Euronet basiert auf der packet-switching Technologie und erlaubt eine möglichst gute Ausnützung der Netzkapazität. Das Netzwerk ist zentral gesteuert: die Leitstelle des Datenübertragungsnetzes befindet sich in London, wobei Paketvermittlungsknoten und Anschlussstellen für den Fernzugriff und die Uebermittlung eingebaut werden. Paketvermittlungsknoten befinden sich in Frankfurt, London, Paris, Rom und Zürich, während Anschlussstellen in Amsterdam, Brüssel, Dublin, Kopenhagen und Luxemburg installiert

156 Vgl. OCDE, Utilisation des Réseaux, S. 216ff. (Netzplan und Konfiguration, S. 217f.).

157 DIANE = Direct Information Access Network for Europe.

158 Tymnet, Telenet usw.

159 Die Rolle der PTT besteht in der Errichtung und Bereitstellung des Fernmeldenetzes.

160 Z.B. die Schweiz: Am 28. Sept. 1979 wurde in Brüssel das Abkommen in Form eines Briefwechsels zur Ausdehnung von Euronet auf die Schweiz unterzeichnet (veröffentlicht im BBl. 1980 I 1001, in Kraft getreten am 28.9.1979). Die Inbetriebnahme des neuen Vermittlungsknotens für das europäische Datennetz erfolgte am 29. Oktober 1980, die offizielle Einweihung fand am 24. November 1980 statt (vgl. BRUDERER, NZZ Nr. 252/1980, S. 36).

161 In der Schweiz ist das Fernmeldedepartement der Post-, Telefon- und Telegrafienbetriebe (PTT) zuständig.

sind.¹⁶² Die Benutzer wählen den nächstgelegenen Knotenrechner ihres Landes, der die Verbindung zum Euronet und der Leitstelle in London herstellt und die Suchabfragen an verschiedene Datenbanken erlaubt.

- Informationsdienste ermöglichen im Endausbau den Zugang zu mehr als hundert verschiedenen Datenbanken, die auf ca. 30 angeschlossenen Computersystemen verteilt sind. Diese Datenbanken gliedern sich derzeit in 80 literaturbezogene (bibliographische) und über 20 sachbezogene (faktische) Datenbasen,¹⁶³ die Millionen von Literaturhinweisen und Informationen zu wissenschaftlichen, technischen, gesellschaftlichen, rechtlichen und sozio-ökonomischen Fragen enthalten,¹⁶⁴ welche aus Europa und den USA stammen. Die Informationsdienste werden von nationalen privaten und öffentlichen Datenbankbetreibern und Informationsanbietern¹⁶⁵ und der EG-Kommission¹⁶⁶ getragen und im Informationsverbund DIANE zur interaktiven Abfrage angeboten.

162 Diese Angaben können sich schnell ändern.

163 BRUDERER, sysdata 11/79, S. 17 (die Zahlen werden rasch überholt sein).

164 Z.B. Astronomie, Bauwesen, Biologie, Chemie, Datenverarbeitung, Elektronik, Elektrotechnik, Energie, Forstwirtschaft, Gemeinschaftsrecht, Hüttenkunde, Informatik, Informationswissenschaft, Landwirtschaft, Lebensmittelkunde, Maschinenbau, Mathematik, Medizin, Meteorologie, Patentwesen, Pharmazie, Physik, Psychologie, Textilwesen, Umweltschutz, etc.

165 Z.B. Blaise Marketing, London; Centro di Calcolo Interfacoltà, Rom; Compagnie Internationale de Service en Informatique, Paris; Ministère des Affaires Economiques, Bruxelles; Datacentralen, Kopenhagen; Deutsches Institut für medizinische Dokumentation und Information, Köln; European Patents Office, Den Haag; Fachinformationszentrum Energie, Physik, Mathematik GmbH, Karlsruhe; EG Kommission.

166 EG Datenbanken, die über ECHO (European Commission Host Organisation) Service in Luxemburg verfügbar sind:

AGREP - Verzeichnis der landwirtschaftlichen Forschungsvorhaben;

EABIS - Literaturangaben und Auszüge zu den von EG finanzierten Studienberichten;

ENDOC - Verzeichnis von Dokumentationszentren und Informationsdiensten im Bereich des Umweltschutzes;

ENREP - Verzeichnis der Forschungsvorhaben im Gebiet des Umweltschutzes;

b) Zielsetzung

Die Wettbewerbsfähigkeit der europäischen Wirtschaft auf der internationalen Handelsebene ist von aktuellen wissenschaftlichen, technischen und wirtschaftlichen Kenntnissen abhängig, was umfangreiche Ausgaben für Information und Dokumentation über Forschung, Entwicklung und andere Bereichen zur Folge hat. Mit Euronet-DIANE soll der kostspielige Aufbau von Datenbanken für einen Informationsaustausch in einem vernünftigen Rahmen gehalten und die Lücke gegenüber dem Datenbankenservice der Vereinigten Staaten geschlossen werden. Euronet ist die Grundlage für ein künftiges öffentliches europäisches Datenübertragungsnetz mit Paketvermittlungstechnologie; die ungenutzte Netzkapazität steht andern, z.B. gewerblichen Zwecken zur Verfügung.¹⁶⁷

Bei der Verwirklichung von Euronet wurde Wert darauf gelegt, die europäische Elektronik- und Fernmeldeindustrie zu unterstützen und zu fördern: Euronet-DIANE besteht heute ausschliesslich aus "europäischer" Hard- und Software.

c) Charakteristika des Euronet-DIANE

- Euronet ist ein speziell entwickeltes Fernmeldenetz mit einem neuartigen Tarif: für die internationalen Uebermittlungsstrecken wurde ein gemeinsamer, distanzunabhängiger Einheitstarif festgelegt, der sich aus der Menge der übermittelten Daten und der Uebertragungsdauer zusammensetzt.
- Die Benutzungsgebühren ergeben sich aus Anschluss und Gebrauch der Teilnehmerrüstungen, aus Benutzung des inländischen Fernmeldenetzes (bis zum Euronet-Anschluss) und des Euronet-Datennetzes sowie aus der Benutzung der Informationsdienste und ihrer Datenverarbeitungsanlagen.

EURODICAUTOM - Terminologiedatenbank für die Gemeinschaftssprachen, etc.

(vgl. BRUDERER, sysdata 11/79, S. 18 und NZZ Nr. 134/1978, S. 15).

167 BRUDERER, sysdata 11/79, S. 18.

- Ausrichtung der Datenbank-Informationen auf europäische Bedürfnisse.
- Zugang zu mehreren europäischen Informationsdiensten über ein einziges Datennetz.
- Benutzerfreundlichkeit dank einheitlicher Dialog- und Abfragesprache. Langfristig sollen die Informationen mittels eines speziellen Uebertragungsverfahrens in mehreren Sprachen zur Verfügung gestellt werden.

d) Natur der Daten

Entsprechend der Zielsetzung von Euronet-DIANE als Datennetz zur optimierten Informationsbeschaffung werden hauptsächlich sachbezogene Daten der verschiedenen Informationsbereiche ¹⁶⁸ ausgetauscht, wobei der Datenschutz, d.h. der Schutz der Privatsphäre, im Rahmen dieses wissenschaftlichen, technischen und wirtschaftlichen Informationsverkehrs eine untergeordnete Rolle spielt. Damit wird auch deutlich, dass personenbezogene Daten im Bereich der Informationsdatenbanken des DIANE keinen Stellenwert haben. Die verfügbaren Informationen sind bereits publiziert und damit auch anders zugänglich oder enthalten nur statistische Angaben: Die Datenbasen dienen der optimierten Informationsbeschaffung angesichts einer ansteigenden Informationsflut.

Nebst der Zielsetzung von Euronet-DIANE als Informationsbeschaffungsmedium wird die ungenutzte Kapazität des physikalischen Datennetzes ändern, z.B. gewerblichen oder kommerziellen Zwecken zur Verfügung gestellt. Im Rahmen dieser offenen Zweckverwendung können sowohl personen- als auch sachbezogene Daten auf dem Netzwerk übermittelt werden; das Ausmass dieses Datenverkehrs ist aber noch nicht abzuschätzen. Euronet ist in diesem Falle ein Ersatz bzw. eine Ergänzung der normalen Telefonleitungen als Transportmedium von Daten.

e) Datensicherung

Die Datensicherung besteht aus einer Reihe von organisatorischen Massnahmen, die einerseits in pragmatischen Vorkehrungen bestehen und ein unbefugtes Zerstören, Verändern, Empfangen und Lesen von Daten

verhindern wie z.B. durch Zutrittskontrolle zu Räumen mit Datenstationen und Computersystemen, Speicherung von Angaben in lesbarer Form oder auf maschinenlesbaren Datenträgern oder in kryptographierter Form auf Speichermedien. Sie werden ergänzt durch technisch-organisatorische Massnahmen, die sich in zwei Bereiche aufgliedern lassen:¹⁶⁹

- Zugriffskontrolle an der Datenstation

Dazu gehören alle Systemeinrichtungen und Vorkehrungen, die nur berechtigten Benutzern Zugang zu den Daten erlauben, wie z.B. Benutzernummer, Passwort, Ausweiskarten usw.; u.U. wird bei erhöhtem Sicherheitsbedürfnis die Nachricht verschlüsselt in der Datenstation gespeichert, damit sie nur für den Inhaber des geheimen Schlüssels zugänglich ist.

- Sicherung der Daten auf dem Uebertragungsweg

Durch Kryptographie, d.h. Verschlüsselung, können die Daten auf ihrem Transport im Netz gegen unbefugtes Lesen oder Aendern gesichert werden. Es gibt hierbei verschiedene Verschlüsselungsverfahren und Techniken, die teils sehr effektiv sind, teils nur geringen Effekt haben; letztere Verfahren werden als "Verschleierung" bezeichnet.

Insofern Euronet-DIANE mit seiner schnellen Uebermittlungstechnologie als reines Uebermittlungsmedium für den gewerblichen, kommerziellen oder administrativen Datenverkehr genutzt wird, stehen grundsätzlich nicht mehr technische Sicherungseinrichtungen als bei gewöhnlichen Telephonleitungen zur Verfügung. Für die Datensicherungskomponenten, wie z.B. entsprechende Software (Identifikationsprozedere, Passwortschutz) und Hardware (Verschlüsselungsgeräte), müssen die betreffenden datenaustauschenden Stellen selbst besorgt sein.¹⁷⁰

168 Vgl. vorne, S. 4, Anm. 13.

169 RAUCH, DS+DS 4/79, S. 242.

170 Hier wird deutlich, dass der Datensicherung eine bedeutende prophylaktische Rolle im physischen Schutz von grenzüberschreitenden Daten zukommt und individuell variieren kann.

Wenn ein Benutzer mit einem Datenbankrechner in Verbindung tritt, sind im zentralgesteuerten Netzwerk und den einzelnen Datenbanken Sicherheitsvorkehrungen vorhanden, die einen unbefugten Anschluss an das Netz einerseits und an eine Informationsdatenbank andererseits, verhindern. Als Sicherungseinrichtungen sind die "user numbers"¹⁷¹ zu nennen, die sowohl von dem nationalen Telegraphenamts beim Erwerb eines Abonnementes zur Benutzung von Euronet ausgegeben, als auch von den Datenbankanbietern beim Vertragsabschluss dem betreffenden Benutzer erteilt werden.¹⁷² Die Geheimhaltung dieser "user numbers" obliegt dem einzelnen Benutzer; weitere Sicherungsmassnahmen (z.B. Passwort) verstärken den Schutz vor allgemeinem Zutritt zum Datennetz oder missbräuchlicher Verwendung einer "user number" durch einen Dritten. In der Netzwerksteuerung und den einzelnen Datenbanken sind ebenfalls Programme eingesetzt, die den Zugang zum Netz registrieren und die Länge der Netzbelastung sowie die Dauer der Rechnerzeit zur Kostenfeststellung¹⁷³ festhalten.

f) Folgerung

Euronet-DIANE wird als physisches Datennetz den Datenverkehr zwischen den europäischen Staaten, d.h. den Mitgliedern der Europäischen Gemeinschaft und den dem Euronet beigetretenen Staaten^{174 175 176}, vergrössern. Die Bedeutung von Euronet für die Schweiz wird vor allem in folgenden Punkten sichtbar werden:

171 Benutzernummern.

172 DIEBOLD MANAGEMENT REPORT, Okt./Nov. 1977, S. 13.

173 In den Gebühren sind ebenfalls die aus dem Urheberrecht entspringenden finanziellen Verpflichtungen enthalten. Der Autor wird aufgrund eines privatrechtlichen Verhältnisses zwischen ihm und der Datenbank nach Anfragehäufigkeiten in seinen urheberrechtlichen Ansprüchen zufriedengestellt.

174 Vgl. Art. 3 des Ratsbeschlusses vom 9. Okt. 1979, (78/887/EWG), in: Amtsblatt der Europäischen Gemeinschaften Nr. 1.311/2.

175 Die Schweiz ist als erster Nichtmitgliedstaat der EG dem Euronet beigetreten.

176 Einen Zugang zu Euronet erwägen ferner: Oesterreich, Schweden, Griechenland und Spanien.

- Mit dem Anschluss wird die Schweiz, die auf Informationsquellen aus dem Ausland angewiesen ist, in den "Freihandel mit wissenschaftlichen und technischen Informationen" der wichtigsten europäischen Industrienationen integriert.¹⁷⁷
- Durch die an Euronet angeschlossenen Informationsdienste und Datenbanken, werden Informationsdienstleistungen angeboten, die mehrheitlich europäischen Ursprungs sind, aber auch amerikanische Datenbanken erschliessen. Dieses europäisch-amerikanische Informationsangebot wird für die amerikanischen Datenbanken und Informationsnetze ¹⁷⁸ eine nicht zu ignorierende Konkurrenz darstellen und einen beträchtlichen Teil der heute über Radio Schweiz AG laufenden Anfragen auf Euronet ziehen. Damit wird die Informationsbeschaffung und Telekommunikation kostengünstiger und das Informationsangebot europäischer (dies kann vor allem im Bereich der sozio-ökonomischen Informationen positive Auswirkungen haben, weil die sozialen und wirtschaftlichen Strukturen in Europa anders gelagert sind als in den USA).
- Die kostengünstige Informationsbeschaffung wird die Zahl der diese Informationsdienste nutzenden Industrie-, Wirtschafts- und Behördenstellen sowie diejenigen der wissenschaftlichen Institute und Forschungszentren anwachsen lassen.
- Nutzen wird aber nicht nur auf der Nachfrageseite gezogen, sondern auch auf der Angebotsseite, indem langfristig, mit zunehmender Datenbanken- und Wirtrechnerzahl (Hauptcomputer, HOST-Computer), sich ebenfalls in der Schweiz Informationsdatenbanken etablieren, die über das Euronet angefragt werden.¹⁷⁹
- Mit der Nutzung des Netzes zu gewerblichen Zwecken wird die Uebermittlung und der Austausch von personen- und sachbezogenen Daten auch für kleinere Unternehmen mit geringem Datenvolumen

177 VON WALTERSKIRCHEN, S. 17.

178 Z.B. Lockheed Information Service, Telenet, Tymnet.

179 Dies bringt zugleich eine Intensivierung der Integration.

attraktiv, da ein Datennetz mit schneller Uebermittlungstechnologie und niedrigen Netztarifen den grenzüberschreitenden Datenverkehr zu stimulieren vermag.

Durch die Unterzeichnung des Abkommens zur Ausdehnung von Euro-net-DIANE auf die Schweiz mit einem Vermittlungsknoten in Zürich, wird nicht nur das Informationsangebot erweitert, sondern auch eine sektorielle Liberalisierung des grenzüberschreitenden Informationsverkehrs geschaffen, die von der Nationalität des Benutzers bedingte Beschaffungskosten vermeidet.¹⁸⁰ Damit "ist es der Schweiz ... gelungen, erstmals das Petitum des ungehinderten Zugangs zu Versorgungsmärkten, das die logische Ergänzung zum bestehenden Freihandel darstellt, in einem völkerrechtlichen Dokument festzuhalten."¹⁸¹

180 Vgl. VON WALTERSKIRCHEN, S. 17.

181 Id., a.a.O.

B. O.I.P.C. - Interpol ^{182 183 184}

a) Anmerkung

Im Gegensatz zu den vorgehend beschriebenen Datennetzen ist dasjenige von Interpol "noch nicht"¹⁸⁵ computerisiert, sondern besteht aus den konventionellen Mitteln des Fernmeldewesens. Der grenzüberschreitende Datenverkehr wickelt sich sowohl über Fernschreiber als auch Funk ab und ist ein lebender Beweis dafür, dass auch mit älteren Technologien - nicht nur mit computerunterstützten Medien - ein extensiver grenzüberschreitender Datenaustausch gepflegt werden kann.¹⁸⁶ Für eine Beschreibung des Interpol-Datennetzes wäre laut Definition der Datennetze ¹⁸⁷ an dieser Stelle kein Raum, doch veranlasst mich die herrschende Diskussion um die Computerisierung von Interpol, und die mit einem Austausch personenbezogener Daten verbundenen Problemkreise, auf das bestehende Interpol-Netz an dieser Stelle einzugehen.

b) Allgemeines

1979 waren 127 Länder der Interpol-Organisation angeschlossen. Gemäss Art. 4 der Statuten ¹⁸⁸ sind die Mitglieder der Organisation die offiziellen Organe der nationalen Polizei, die von ihren eigenen Ländern bestimmt werden und als Verbindungsglied zwischen den lokalen, regionalen oder nationalen Polizeistellen und dem Interpol-Generalsekretariat stehen. Die Zusammenarbeit der Polizei innerhalb der Interpol ist offizieller Natur, obwohl sie nicht auf einer internationalen Konvention, sondern auf zwischenstaatlichen völkerrechtlichen Verträgen und den Statuten der Interpol beruht; auch von den Vereinigten Nationen wird Interpol als "Intergovernmental Organisation" anerkannt.

182 O.I.P.C. = Organisation internationale de Police Criminelle.

183 SCHLANITZ, OECD-ICCP1, S. 102ff.

184 Vgl. OCDE, Utilisation des Réseaux, S. 190ff.

185 Die Umstellung auf ein EDV-gestütztes Datennetz ist geplant.

186 Vgl. vorne, S. 1, Anm. 1.

187 Vgl. vorne, S. 49 und Anm. 3.

188 INTERPOL, Constitution.

c) Zweck

Der Zweck besteht gemäss Art. 2 der Statuten in der Sicherstellung und Entwicklung der grösstmöglichen gegenseitigen Hilfeleistung aller Kriminalpolizeibehörden im Rahmen der bestehenden verschiedenen nationalen Gesetze¹⁸⁹ und entsprechend dem Sinn der Allgemeinen Menschenrechtsdeklaration, ferner in der Schaffung und Förderung von geeigneten Institutionen zur Vorbeugung und Vermeidung von allgemeinen Rechtsverletzungen. Art. 3 der Statuten untersagt Interpol aber absolut jede Tätigkeit oder Eingriffe bei Strafsachen, die politischen, militärischen, religiösen oder rassistischen Charakter haben.

Zur Verwirklichung ihrer Ziele benötigt die Organisation eine kontinuierliche, aktive Zusammenarbeit der Mitglieder, die alle national gesetzeskonforme Anstrengungen zur Teilnahme an der Organisation unternehmen müssen.

Die wesentliche Haupttätigkeit der Organisation besteht im Austausch polizeilicher Informationen über Verbrechen und Rechtsdelinquenten zwischen den Mitgliedstaaten.

d) Struktur und Aufbau des Interpol-Netzes

aa) Auf internationaler Ebene besteht ein Generalsekretariat, das als internationales Informationszentrum in der Kriminalitätsbekämpfung fungiert und zu diesem Zweck manuelle Dateien mit einem Umfang von über 2'700'000 Personenregisterkarten und ca. 150'000 Fingerabdruckkarten¹⁹⁰ über Verbrecher bzw. gesuchte, unter Arrest oder Haft stehende Personen nachführt.

bb) Auf nationaler Ebene bestimmt jedes Land eine Polizeistelle, die als nationales Zentralbüro operiert und sowohl mit den innerstaatlichen Polizeibehörden und Ermittlungsbeamten als auch mit ausländischen nationalen Zentralbüros und dem Generalsekretariat Verbindung unterhält und Daten austauscht. Diese nationalen Zen-

189 Die Schweiz erteilt aber gemäss langjähriger Praxis keine Rechtshilfe in Fiskalstrafsachen.

190 TDR, Vol. 2, No. 2, S. 13; OCDE, a.a.O., S. 192.

tralbüros bleiben Bestandteil der nationalen Verwaltungsstruktur der einzelnen Länder.

- cc) Die Verbindung zwischen Generalsekretariat und einem Teil der nationalen Zentralbüros wird durch ein autonomes Fernmeldeverkehrsnetz (Telex und Funk) sichergestellt; daneben findet aber immer noch die traditionelle Kommunikation auf dem Postwege statt.

Die Struktur des Datennetzes ist hier einerseits sternförmig, gebildet durch die Hierarchie Generalsekretariat - nationale Zentralbüros, andererseits besteht auch eine Verbindung direkt unter den nationalen Zentralbüros. Entscheidend ist, dass im Generalsekretariat die Angaben jedes Landes zentral gespeichert und von dieser Stelle auch koordiniert weitergegeben und nachgeführt werden.

e) Natur der Daten

Die Informationen der einzelnen Stellen betreffen Verbrecher und Verbrechen. Die Daten beziehen sich hauptsächlich auf international gesuchte Personen sowie auf charakterisierende Sachverhalte bzw. identifizierbare Tathergänge hinsichtlich von Personen, die bei der internationalen Verbrechensbekämpfung in Erscheinung treten.

Die Daten sind somit hauptsächlich personenbezogener, aber auch sachbezogener Natur, wie:

- Name, Geburtsdatum, Geburtsort;
- Beschreibung der Person mit besonderen Erkennungszeichen;
- Fotografie;
- Fingerabdrücke;
- Vorstrafen- und Strafregister;
- Arbeitsort;
- Angaben zur psychischen und geistigen Verfassung als Illustration der Gefährlichkeit;
- Neigungen und Interessen;
- Beschreibung des Sachverhalts eines Verbrechens;
- Tatvorgänge (modus operandi) u.a.m.

Die Informationen enthalten nie Angaben zur politischen und religiösen Ueberzeugung oder Tatsachen des Privatlebens, die nicht im Zusammenhang mit der Strafuntersuchung und -verfolgung stehen.

f) Informationsfluss

Die auf Delinquenten und ihre Rechtsverletzungen bezogenen Daten werden auf verschiedenen Kanälen übermittelt:

- aa) Innerhalb der Organisation: zum einen Teil zwischen den nationalen Zentralbüros und dem Generalsekretariat, zum andern Teil direkt zwischen den nationalen Zentralbüros; innerhalb der Organisation ist der Datenaustausch praktisch immer grenzüberschreitender Natur.
- bb) Ausserhalb der Organisation gibt es in der Regel ¹⁹¹ keinen transnationalen Datenverkehr von Interpol-Angaben, da jedes nationale Zentralbüro die Daten nur den innerstaatlich zuständigen Polizei- und Ermittlungsbehörden weiterleitet.

Die Bemühungen, im Interpolbereich eine Statistik zu schaffen, stossen in einzelnen Ländern ebenso auf Schwierigkeiten wie die geplante Errichtung eines Computersystems für Personendaten. Es sei deshalb nur am Rande und anhand unvollständiger Statistiken ¹⁹² erwähnt, dass 1977 zwischen den wichtigsten nationalen Zentralpolizeibüros der Interpol, welche eine Statistik geliefert haben, 329962 Meldungen ausgetauscht wurden. Im Jahre 1977 betrug die Zahl der Funk- und Telexmeldungen, die Interpol Schweiz empfang oder absetzte, 48185. ¹⁹³

¹⁹¹ Es existiert aber auch noch ein sog. 'kleiner grenzüberschreitender Datenverkehr', der nicht den Austausch von Interpolangaben, sondern Daten der nationalen, z.T. benachbarten Polizeidienststellen beinhaltet. Da es aufgrund der BV Sache des Bundes ist, die Schweiz nach aussen zu vertreten, wenden sich die kantonalen und städtischen Kriminalpolizeistellen bei internationalrechtlichen Tatbeständen an Interpol Schweiz.

¹⁹² SCHLANITZ, OECD-ICCP1, S. 104.

¹⁹³ Tagesdurchschnitt von 132 ein- und ausgehenden Meldungen.

Die Uebernahme der Personenregisterkarten auf ein Computersystem ist schon lange geplant, die Verwirklichungsphase wird jedoch durch die mit der Beschaffung der Systeme zusammenhängende Problematik stets verzögert.¹⁹⁴ Die Bestellung eines zweiten Computersystems, das dem Aufbau eines Netzes dienen sollte, und mit dem durch die elektronische Ausstattung einiger nationaler Zentralbüros der direkte Anschluss an das Generalsekretariat geschaffen würde, ist infolge möglicher datenschutzrechtlicher Unvereinbarkeiten in Frage gestellt. Geplant ist ein autonomes System und Netz, das unabhängig von existierenden nationalen Systemen¹⁹⁵ betrieben werden kann, um die Vertraulichkeit der Daten sicherzustellen.

g) Datenschutz

Die Statuten überlassen das Ausmass der Zusammenarbeit der Normierung durch die Gesetze der Mitgliedsländer und bestimmen, dass kein nationales Zentralbüro irgendeinem andern Zentralbüro bzw. dem Generalsekretariat Informationen liefern oder übermitteln darf, wenn dies einen Bruch des eigenen Landesrechts darstellen würde (Legalitätsprinzip). Das Generalsekretariat ist verpflichtet, die Behandlung von kriminalpolizeilichen Nachforschungen durch die nationalen Zentralbüros ausführen zu lassen und kann deshalb diesem nur die die Individuen betreffenden Daten übermitteln. Nach Empfang von Angaben durch das nationale Zentralbüro unterliegen diese der entsprechenden nationalen Rechtsordnung; die einzelnen Mitgliedstaaten tragen somit die Verantwortung für den Schutz der Daten und die Wahrung der Interessen der Betroffenen, ebenso bei einer Weitergabe der Informationen auf nationaler oder internationaler Ebene. Der Daten- und Interessenschutz dieser nationalen Polizeizusammenarbeit obliegt somit in erster Linie den Dienststellen und Behörden eines Landes, die solche

194 Vgl. TDR, Vol.2, No.2, S. 5/13; ferner TDR, Vol.2, No.3, S. 15.

195 Z.B. das geplante KIS (kriminalpolizeiliches Informationssystem): vgl. NZZ Nr. 156 vom 8./9. Juli 1978 und Nr. 289 vom 12. Dez. 1979.

196 Wenn z.B. ein nationales Zentralbüro die Daten in einem Computer speichert, unterliegen diese der nationalen Rechtsordnung, d.h. auch einem Datenschutzgesetz oder -bestimmungen, falls solche vorhanden sind.

Informationen im Rahmen der Kooperation empfangen und mit ihr arbeiten. Das Generalsekretariat ist für angemessene Sicherungsmassnahmen der Daten verantwortlich: dies umfasst sowohl die zentrale Speicherung als auch die Uebermittlungen auf dem Fernmeldenetz oder per Post - wenn notwendig, muss diese Uebertragung in verschlüsselter Form erfolgen.

Der spezielle Charakter der Daten, die das Generalsekretariat und die nationalen Zentralbüros speichern, erfordern einen absoluten Schutz gegen Missbrauch der gespeicherten personenbezogenen Informationen. Deren Vertraulichkeit liegt nicht nur im Interesse der zu wahrenen Persönlichkeitsrechte, die durch Vorschriften des materiellen Rechts garantiert sein sollten, sondern auch i.S. der polizeilichen Aufgaben im Rahmen der Durchführung von Untersuchungen und Nachforschungen. Die Bestimmungen des Berufs- und Amtsgeheimnisses sowie diejenigen der Strafprozessordnungen tragen ebenfalls zur Verstärkung des Schutzes von personenbezogenen Daten bei. Nur in bestimmten Fällen erfolgt eine Preisgabe des Schutzes einzelner Daten, wenn zwecks Zusammenarbeit mit der Bevölkerung gewisse Daten und Angaben von Verbrechern veröffentlicht werden.

Es ist interessant, festzustellen, dass in diesem mit vertrautem Mitteln (Telex, Funk und Post) geführten Datenaustausch über die nationalen Grenzen hinweg praktisch nie von Persönlichkeitsverletzungen zu hören ist. Dabei ist zu bedenken, dass die Zusammenarbeit der Polizeibehörden Personen betrifft, die durch ihr rechtsverletzendes Verhalten Voraussetzungen geschaffen haben, die diesen nicht im gleichen Umfang einen Anspruch auf Schutz ihrer personenbezogenen Daten gewähren, wie den übrigen Rechtsgenossen. M.E. haben sich die bestehenden Bestimmungen zum Schutz von Daten im Informationsaustausch mit herkömmlichen Mitteln und Medien bewährt und bilden eine gute Voraussetzung für die mit einer Umstellung auf automatisierte Datenverarbeitungssysteme und ein computerisiertes Netzwerk notwendigen datenschutzrechtlichen Ergänzungen und Aenderungen. Bei der

Regelung des grenzüberschreitenden Datenverkehrs darf deshalb nicht ausser Acht gelassen werden, dass verschiedene Rechtshilfe- und Auslieferungsabkommen den Austausch derartiger Daten auf der Stufe eines Staatsvertrages verlangen.

h) Folgerung

Auch hier wird deutlich, dass mit einer Digitalisierung der bestehenden Personenkarteien und Computerisierung des Datennetzes eine alte Aufgabe mit neuen Mitteln zu lösen versucht wird, um eine bessere und wirksamere Verbrechensbekämpfung durch aktuellere Informationen zu erreichen.

Eine konzise Bestimmung des Speicherumfanges der Daten, die angesichts unbegrenzter Speicherungsmöglichkeiten nicht von einem hypertrophen Informationsbedürfnis beeinflusst sein darf, und eine klare, absolute Trennung des Interpol-Computersystems und -Datennetzes von nationalen Polizeinformationssystemen¹⁹⁷ (eventuell durch entsprechende Datensicherungsmassnahmen) könnten eine Eskalation der Protestwelle in der Öffentlichkeit wegen vermeintlicher Bedrohung der Freiheitsrechte durch nationale und internationale Polizeiorgane vermeiden helfen.

Mit einer Computerisierung des Interpol-Datennetzes sind aber auch datenschutzrechtliche Aspekte und Probleme zu lösen:¹⁹⁸

- Aus der Tatsache, dass die nationalen Datenschutzbehörden mit unterschiedlichen Einsichts- und Kontrollbefugnissen gegenüber personenbezogenen Datenbanken von Computersystemen öffentlicher Stellen, wie z.B. Polizeibehörden, ausgestattet sind, werden diejenigen Datenschutzbehörden mit beschränkten Einsichtsrechten versuchen,

197 Eine Verbindung von nationalen Polizeicomputern mit dem Interpolsystem kann sich wegen des national unterschiedlichen Speicherungsumfanges als schwierig erweisen. Die gleiche Problematik stellt sich bei einer Verbindung der nationalen Polizeicomputer untereinander: der Speicherungsumfang von England erscheint rudimentär gegenüber dem komplexen Aufbau des BKA-Computers in der Bundesrepublik (vgl. HALLET, OECD-ICCP1, S. 107ff).

198 Vgl. Ausführungen von RIEGEL, in TDR, Vol. 2, No. 3, S. 15.

ihre nationalen Bestimmungen auch auf die von Interpol gespeicherten Daten auszudehnen, damit ausländische Stelle nicht weitergehende Rechte haben als sie selbst.

- Restriktionen des grenzüberschreitenden Datenverkehrs in nationalen Gesetzen können den für die Funktionsfähigkeit von Interpol notwendigen Datenaustausch hemmen: Laut Art. 2 der Statuten sind die Mitgliedstaaten bzw. die Polizeiorgane verpflichtet, die kriminalpolizeilichen Behörden anderer Staaten bei der Vorbeugung und Verfolgung von Rechtsverbrechen zu unterstützen; die Erfüllung dieser Verpflichtung zur Zusammenarbeit bedingt gemäss Legalitätsprinzip die Anwendung des nationalen Rechts. In der BRD z.B. entsteht nach § 11 BDSG die Situation, dass das deutsche Zentralbüro für alle deutschen Daten, die sich im Interpol-System befinden, verantwortlich ist und diese auch kontrollieren können sollte, während nach der bestehenden Rechtslage das Bundeskriminalamt zuständig ist für Änderungen, Sperrung oder Löschung von Daten, die ins Ausland übermittelt werden.¹⁹⁹ Inkompatibilitäten von Bestimmungen auf nationaler Ebene müssen vermieden werden, damit die Verpflichtung nach Art. 2 der Interpolstatuten erfüllbar bleibt.

Daraus ergeben sich folgende Postulate:

- aa) Bei Unvereinbarkeiten und Gesetzeskonflikten dieser Art müssten m.E., in den Statuten der Interpol - im Hinblick auf deren Funktionsfähigkeit - Ausnahmebedingungen geschaffen werden, die dem nationalen Recht nicht grundsätzlich den Vorrang gegenüber diesen Statuten gewähren. In die Statuten sollten vielmehr Datenschutzbestimmungen aufgenommen werden, die bei formeller Inkompatibilität mit dem nationalen Datenschutzrecht eine Ausweglösung zugunsten der Funktionsfähigkeit von Interpol vorsehen. Bei materiellen Rechtsdifferenzen oder dem "ordre public" zuwiderlaufenden Bestimmungen der Interpol-Statuten sollte das nationale Recht hingegen weiterhin Vorrang haben.

199 Id., a.a.O.

In formeller Beziehung müssten die Statuten eindeutig festlegen, dass keiner andern Organisation oder Behörde, ausser der nationalen Kriminalpolizei, Zugang zum Datennetz gewährt wird; eine Einsichtsberechtigung in die Dateien von Interpol wäre nur einer unabhängigen, überstaatlichen, für Interpol zuständigen Datenschutzbehörde gestattet. Für bestimmte Ausnahmefälle könnte man den einzelnen nationalen Datenschutzbehörden ein Einsichtsrecht im Einvernehmen mit dem Generalsekretariat zugestehen.

- bb) In den Bestimmungen ²⁰⁰ sollte ebenfalls festgelegt werden, dass jede nationale Polizeibehörde, die über die nationale Zentralstelle von Aenderungen, einer Sperrung oder Löschung von Daten Kenntnis erhält, die entsprechende Benachrichtigung auch tatsächlich weiterleitet und vollzieht.
- cc) M.E. zeigt sich, dass in einer internationalen Vereinbarung Spezialbestimmungen ²⁰¹ aufgenommen werden sollten, die bereichsspezifische Grundsätze für die speziellen Tätigkeiten und Datenverarbeitungsbedürfnisse einer solchen internationalen Organisation enthalten sollte. Damit wird nicht nur dem Datensubjekt ein Schutz verliehen, sondern auch eine Rechtsgrundlage für die internationale Zusammenarbeit der nationalen Behörden von Mitgliedstaaten mit dem Generalsekretariat nach den in einer Konvention statuierten Prinzipien geschaffen.
- dd) Als einzige materielle, i.S. der EMRK und der Allgemeinen Deklaration der Menschenrechte durch die Vereinten Nationen jedoch vertretbare Bestimmung sollte den betroffenen Datensubjekten in

200 Hier sollten die Statuten eine entsprechende Vorschrift in den nationalen Polizei-Verordnungen voraussetzen.

201 Auch dieses Postulat unterstreicht die Bedeutung einer internationalen Konvention und deren Möglichkeit, die anders gelagerten Bedürfnisse und speziellen Anforderungen allgemein anerkannter internationaler Organisationen (wie z.B. Interpol, UNO) u.U. in einem speziellen Teil zu berücksichtigen oder zumindest die Grundprinzipien des Datenaustausches nationaler Stellen mit internationalen Behörden auszuarbeiten (vgl. hinten, S. 410ff.).

allen Mitgliedstaaten von Interpol vergleichbare Rechte zustehen, denn auch hier gilt es, das Individuum als Persönlichkeit zu respektieren.

Das Ausmass des mit einfachen Mitteln der Telekommunikation betriebenen Datenverkehrs und die Bedeutung eines intensivierten Austausches von kriminalistischen Angaben und Daten im internationalen Polizeibereich reflektiert die Internationalisierung der Kriminalität mit ihren multinationalen Verzweigungen, der nur durch transnationale Zusammenarbeit der Polizeistellen begegnet werden kann. Bei einer wirksamen Bekämpfung der modernen, organisierten Formen der Kriminalität werden die internationalen Polizeibehörden in der Zukunft nicht ohne computerisiertes Datennetz und intensiven, koordinierten Datenaustausch auskommen. Angesichts dieser Tatsache wird jede Beschränkung, die einem freien internationalen Austausch derartiger Daten auferlegt wird, das internationale Verbrechen begünstigen und den gemeinsamen Interessen aller Rechtsstaaten zuwiderlaufen.²⁰²

202 SCHLANITZ, OECD-ICCP1, S. 105.

III. Andere Formen der Datenübermittlung

Die Aufzählung verschiedener Träger von Datennetzen soll nicht zur Annahme verleiten, dass diesen alleine, aufgrund einer Netzinfrastruktur, der grenzüberschreitende Datenverkehr und die Verarbeitung von Daten im Ausland möglich wäre. Die Beschreibung von Datennetzen und ihrer Träger, beschränkt sich hier auf einige wenige bekannte und wichtige.²⁰³

Zur Uebermittlung von Daten zwischen zwei Stellen in verschiedenen Ländern bedarf es nicht unbedingt einer Netzstruktur, vielmehr genügt eine einzige Verbindung,²⁰⁴ z.B. via Satellit, Wahl- oder Mietleitung, zwischen den kommunizierenden Computersystemen bzw. Datenstationen. In der Praxis hat diese Erscheinungsform einen beträchtlichen Anteil am grenzüberschreitenden Datenverkehr, weil hauptsächlich im privaten,²⁰⁵ vereinzelt aber auch im öffentlichen²⁰⁶ Sektor eine Anzahl nationaler, voneinander unabhängiger Institutionen, die miteinander einen grenzüberschreitenden Datenverkehr unterhalten,²⁰⁷ über eine solche point-to-point - Verbindung kommunizieren.

Volumenmässig nicht zu unterschätzen ist der Austausch computerisierter Daten ohne Telekommunikationsmittel, d.h. auf dem traditionellen Post- und Versandweg mittels geeigneter Datenspeichermedien in Form von Bändern, Disketten, Magnetkarten, Lochkarten oder sogar Magnetplatten.²⁰⁸ Die Uebermittlung solcher teils roher, teils maschinenlesbarer Daten zur Verarbeitung wird oft vorgenommen, wenn

203 Für weitere Datennetze vgl. OCDE, Utilisation des Réseaux.

204 Sog. point-to-point-connection.

205 Z.B. verschiedene Kreditversicherungsgesellschaften, Joint Ventures: BASTIN, OECD-ICCP 1, S. 127ff.

205 Z.B. Sozialversicherungs- und Steuerwesen: O'CONNOR, OECD-ICCP1, S. 92ff.

207 Der Datenaustausch kann aber auch zwischen privaten und öffentlichen Stellen stattfinden, wie dies vor allem mit wissenschaftlichen und statistischen Daten erfolgt.

208 Vgl. MORAN, OECD-ICCP 1, S. 98ff. "...there is significantly more data flowing into and out of the country on magnetic media than via telecommunication.", ebenso FREESE, Data Flow, S. 25.

zwischen zwei Computersystemen eine Verbindung über einen physischen Datenträger aus technischen Gründen nicht möglich ist oder aus andern Ueberlegungen²⁰⁹ nicht opportun erscheint. Für die zahlreichen Stellen,²¹⁰ die Daten auf solchen Speichermedien zum Verkauf anbieten, ist der Versand die übliche Form des Datenverkehrs.

Zusammenfassend muss aber festgestellt werden, dass unter allen Formen der Datenübermittlung dem Datenverkehr über die gemeinschaftlichen und privaten Datennetze gegenwärtig eine bedeutende Stellung zukommt. In naher Zukunft wird der Stellenwert des auf Datennetzen erfolgenden genzüberschreitenden Informationsflusses noch weiter zunehmen, weil öffentliche bzw. allgemein zugängliche internationale und nationale²¹¹ Datennetze zur Verfügung stehen und höhere Uebertragungsgeschwindigkeiten²¹² aufweisen als die regulären Telephonleitungen, die zur Datenübermittlung mit Wahl- und Mietleitungen benutzt werden. Die schnellere Uebermittlung und die Kostenberechnung nach anteilmässiger Benutzung des Datennetzes machen den grenzüberschreitenden Datenverkehr kostengünstig und die daraus fliessenden Vorteile (z.B. Konsolidierung oder Ausnützung fremder Hardware-/Software- Kapazität) für viele Unternehmen und Institutionen attraktiv.²¹³ Diese Tatsache wird den grenzüberschreitenden Datenverkehr während der kommenden Jahre zu einem gewichtigen Faktum und Diskussionspunkt in den internationalen Datenschutzbestrebungen machen.

209 Z.B. zu hoher Kostenaufwand für Modems, Miet- oder Wahlleitungen u.a.

210 So bieten die PTT-Betriebe die Telephonbücher nicht nur in der üblichen Buchform zum Verkauf an, sondern auch als Datenbestand auf Bändern; hier ist z.B. an die Firmen zu denken, die im Auftrage von Dritten Datenbanken erstellen und diese laufend nachführen (was datenschutzrechtlich nicht ohne Probleme ist).

211 Die nationalen Datennetze werden über Protokolle mit andern nationalen Netzen verbunden sein, so dass diesen nicht nur der nationale Datenfluss vorbehalten bleibt.

212 Gleich wie die privaten und gemeinschaftlichen Netzwerke.

213 Vgl. auch OCDE, Utilisation des Réseaux, S. 23ff.

Ein Datenschutzgesetz bzw. eine internationale Vereinbarung sollte alle Formen des grenzüberschreitenden Datenverkehrs, sowohl diejenigen der Telekommunikation als auch die herkömmliche Uebermittlung,²¹⁴ erfassen, wenn sie nicht mit einfachen Methoden umgangen werden sollen. Besonders bedeutungsvoll ist diese Forderung z.B. für eine Konvention, in der alle Mitgliedstaaten darauf angewiesen sind, dass bei keinem Mitglied ein "Datenleck" herrscht, aus dem Daten aus dem Hoheitsbereich der Konventionsstaaten in "data havens" fließen.

IV. Arten von Daten, die den grenzüberschreitenden Verkehr bilden

1. Klassierung²¹⁵

Im Auftrag der OECD war die englische Firma Logica Ltd. an einer Ausarbeitung einer Studie beteiligt und erhielt dadurch Einblick²¹⁶ in verschiedene internationale Datennetz-Anwendungen, die eine bereichsspezifische Klassierung²¹⁷ der Daten des grenzüberschreitenden Verkehrs erlaubt.

A. Im privaten Bereich

Der Anteil des Transfervolumens aus dem privaten Bereich ist bedeutend grösser als der des öffentlichen Sektors. Davon haben wirtschaftliche und technische Daten den grössten Prozentsatz.

a) Daten der Produktions- und Vertriebskontrolle

Anwendungen im Bereich der Auftragsverarbeitung, der Produktionskontrolle, des Vertriebs, Verkaufs und der Wartung werden von grossen

214 Vgl. vorne, S. 46f.

215 JOHNSON, Online, S. 163ff.

216 Ein Resultat dieser Betrachtungen ist die Publikation der OECD: Utilisation des Réseaux Internationaux de Transmission des Données en Europe, vgl. a.a.O., S. 3.

217 Die Einteilung kann aber nicht als abschliessend betrachtet werden; vgl. auch SCHWAPPACH, DS+DS 1/78, S. 22.

Gesellschaften der verschiedensten Branchen^{218 219} auf internationaler Ebene angewandt und haben eine internationale Uebermittlung von Produkte- und Bestelldaten, teilweise auch mit Kundenangaben zur Folge. Diese gemischten (sach- und personenbezogenen) Datenflüsse sind vor allem denkbar, wenn eine Bestellung an eine Produktionsstätte ins Ausland erfolgt, bei Garantiefällen die zuständige Stelle sich im Ausland befindet oder ein Stammhaus die Daten aller Kunden produktionsspezifisch sammelt, um bei Rückrufaktionen wegen Mängel eine schnellere und zentrale Durchführung zu ermöglichen.²²⁰

Kundendaten sind hier volumenmässig nicht so bedeutend wie wirtschaftliche und technische Informationen, sind aber doch recht häufig. Daten der Vertriebskontrolle können zum Teil Lieferanten betreffen, die meist juristische Personen oder Einzelunternehmen sind; sie werden nur dann an andere Stellen übermittelt werden müssen, wenn Unregelmässigkeiten beim Transport auftreten, so dass personenbezogene Informationen an die zuständigen Stellen ins Ausland weiterzuleiten sind.

b) Daten der finanziellen Bewirtschaftung und Planung

Grosse multinationale Unternehmen verwenden die Datennetze zur finanziellen Koordination und Konsolidierung auf ähnliche Weise wie im Bereich der Produktionskontrolle. Auch im Rahmen der Investitions- und Finanzplanung werden gesellschaftsintern erarbeitete Daten über Planungsapplikationen mit Hilfe von Wirtschaftsindikatoren und Angaben aus öffentlichen Datenbanken²²¹ konsolidiert. Diese Planungs- und Wirtschaftsdaten sind in der Regel für die einzelnen Unternehmen von höchster Wichtigkeit und können bei Indiskretionen in einer Verletzung des Geschäftsgeheimnisses resultieren.

218 Chemie und Mineralindustrie, Elektronik-Industrie, Maschinen- und Automobilindustrie, usw.

219 Vgl. vorne, S. 85ff.

220 SCHWAPPACH, DS+DS 1/78, S. 22.

221 Z.B. OECD-Datenbank: MEI = Main Economic Indicators.

c) Daten über Arbeitnehmer und Gehaltsabrechnungen

Personenbezogenen Daten über Arbeitnehmer werden weniger oft international übermittelt als vermutet wird, weil das Bedürfnis nach internationaler Koordination im Personalbereich (Personalbedarfs- und -einsatzplanung, Aus- und Weiterbildung, Beförderung) zwar vorhanden,²²² - vor allem aus Gründen der personellen Kapazitätsstreuung (meist wird es sich hier um Führungskräfte handeln), - aber nicht dominant ist. Bei Konsolidierung von Personaldaten spielt die Individualität eine untergeordnete Rolle, so dass der Privatsphäre des einzelnen kaum Verletzungsgefahr droht, da die Masse der Informationen jeden individuellen, identifizierbaren Bezugspunkt untergehen lässt.

d) Daten finanzieller Transaktionen

Bankmitteilungen, Krediterteilung und damit zusammenhängende Informationen stellen einen bedeutenden Anteil des internationalen Informationsflusses und speziell der ausgetauschten sensitiven Daten. In der Regel verbleiben die Angaben zur Kreditwürdigkeit bei der vertragsschliessenden Stelle und gelangen erst in den internationalen Verkehr, wenn Insolvenzen grösseren Umfanges zu Tage treten. Ein hoher Stand an Sicherheitsvorkehrungen und gesetzlichen Vorschriften (z.B. Bankgeheimnis) gewährleistet die für den internationalen Handel wichtigen Informationen und deren Datensicherheit.

e) Reisereservationsdaten

Daten in Form von Flugreservationen,²²³ die meistens mit anderen Reiseinformationen verbunden werden, sowie Frachtangaben bilden wahrscheinlich die grösste Einzelkomponente im grenzüberschreitenden Datenverkehr.

222 Vgl. vorne, S. 12, Anm. 18: Fall SIEMENS.

223 Vgl. vorne, S. 55ff.

f) Daten der Marktbeobachtung und -analyse ²²⁴

Daten zur Marktanalyse werden in der Regel aus Gründen der Ortsnähe von den am Ort bzw. in der Region ansässigen Unternehmen oder Niederlassungen (bei Konzernen) im Ausland durchgeführt. Die oft beträchtliche Zahl der gesammelten personenbezogenen Informationen verlassen nur sehr selten das Inland, weil sie meistens in anonymisierter, statistischer Form an eine zentrale Stelle zur Auswertung übermittelt werden, wenn eine Marktanalyse überhaupt auf internationaler Ebene durchgeführt wird. Gesellschaften jeder Grösse bedienen sich bei Marktbeobachtungen der lokalen bzw. regionalen Beratungsfirmen, die die Ergebnisse der personenbezogenen Daten wegen ihrer Aussagekraft auch nur in statistischer Form vorlegen; Einzelangaben sind in Fällen der Marktanalyse nicht von Interesse und dienen u.a. dem Wahrheitsbeweis von Umfragen.

Für Werbung und Direktversand ist in grösseren Sprachräumen mit verschiedenen Ländern ein geringer grenzüberschreitender Fluss von Daten zu registrieren.

B. Im öffentlichen Sektor

Dies ist ein schwer zu analysierender Bereich; er ist aber mit Sicherheit noch nicht sehr bedeutungsvoll in seinen Ausmassen. Doch muss beachtet werden, dass in diesem Sektor die transferierten Informationen i.d.R. personenbezogener Natur sind.

a) Daten von Regierungsstellen und öffentlichen Behörden

Da die meisten Behördenstellen ²²⁵ mit personenbezogenen Daten beschäftigt sind, ist im nationalen Bereich sehr stark auf eine Beschränkung der Informationsmöglichkeit zwischen den einzelnen Behördenstellen zu achten. Im internationalen Bereich ist die supranationale Kooperation mit personenbezogenen Daten ausser bei Interpol

224 SCHWAPPACH, DS+DS 1/78, S. 22.

225 Z.B. Steuerwesen, Einwohnerkontrolle, Sozialversicherung, Polizei, usw.

noch nicht sehr stark ausgeprägt, aber in einigen wenigen Bereichen bereits existent;²²⁶ der transnationale Datenfluss wird aber hier mit verstärkter internationaler Zusammenarbeit anwachsen.

b) Daten der wissenschaftlichen Forschung und Entwicklung

Der Umfang an Daten dieses Bereiches darf nicht unterschätzt werden: Gerade bei Forschung und Entwicklung ist es ein spezifisches Anliegen, erarbeitete und bekannte, dokumentierte Versuche einem größeren Bereich zugänglich zu machen. Mehrere europäische Forschungszentren betreiben deshalb zur Arbeitserleichterung internationale Zusammenarbeit und einen Informationsaustausch untereinander. In diese Kategorie gehören ebenfalls die Anfragen an Informationsdatenbanken (vgl. DIANE).²²⁷ Im innergesellschaftlichen Datenaustausch der Laboratorien multinationaler Gesellschaften²²⁸ können diese wissenschaftlichen Forschungsdaten höchst sensibler Natur sein.

c) Medizinische Daten

Charakteristikum ist ihr besonders sensibler Gehalt. Nicht nur für die direkte medizinische Betreuung von Datensubjekten, sondern auch im Zusammenhang mit der Forschung und Entwicklung neuer Produkte in der Pharmaindustrie, bei Versicherungsgesellschaften, der Sozialversicherung, Krankenkassen, internationalen Organisationen (z.B. Drogenbekämpfung) sowie innerhalb der wissenschaftlichen Forschung ist ein grenzüberschreitender Fluss dieser Daten zu beobachten.

d) Daten der Umweltüberwachung

Als Beispiel kann hier die Welt-Wetter-Überwachung (WMO) genannt werden, die die Verteilung der meteorologischen Angaben für die Wettervorhersage, Flugdienste und Katastrophenprävention verwendet.

226 Einige wenige Behördenstellen lassen statistische und administrative Informationen im Ausland verarbeiten, andere pflegen auf bestimmten Gebieten einen gezielten Datenaustausch: z.B. BRD-CDN im Bereich der Sozialversicherung.

227 Vgl. vorne, S. 101ff.

228 Vgl. vorne, S. 79ff.

Aehnliche Anwendungen werden auch in anderen Bereichen, wie Ueberwachung der Umweltverschmutzung, realisiert.

2. Umfang

Einen allgemeinen zahlenmässigen Umfang des grenzüberschreitenden Datenverkehrs und der Verarbeitung der Daten im Ausland festzulegen, ist nicht möglich, noch weniger eine Verhältniszahl des Anteils der verschiedenen Bereiche. Es existieren nur vereinzelt netzspezifische Angaben und Statistiken, wie z.B. bei SITA²²⁹ und SWIFT.²³⁰ Allgemein kann eine Praeponderanz des Anteils sachbezogener Informationen gegenüber personenbezogener Daten festgestellt werden.²³¹ Informationen von grossen Netzwerkbetreibern ergeben als Datenaustauschvolumen eine Zahl zwischen 1 Milliarde und 100 Milliarden Zeichen pro Jahr. Das immense Geschäftsvolumen solcher Gesellschaften rechtfertigt auch den Betrieb eines eigenen Datennetzes; die grosse Zahl an Benützern mit kleinerem Datenumsatz wird durch die Bereitstellung öffentlicher Datennetze (zu erschwinglichen Kosten) das Volumen des grenzüberschreitenden Datenverkehrs in den nächsten Jahren beträchtlich anwachsen lassen.

3. Konsequenz

Das Resultat dieser Einteilung führt u.a. zur Feststellung, dass die Daten als solche, gleichgültig aus welchem Bereich sie stammen, nicht gefährlich sind, sondern erst durch die Sachaussage im Kontext und dem Interpretieren derselben ein Persönlichkeitsrecht zu verletzen vermögen. Eine Verletzung der Persönlichkeitsrechte natürlicher und juristischer Personen kann nun aber sowohl durch personen- als auch durch sachbezogene Daten erfolgen, so dass die Beschränkung des Schutzes auf die Privatsphäre gemäss der Sphärentheorie nicht genügend ist, sondern alle Daten geschützt werden sollten, die ein

229 Vgl. vorne, S. 55ff.

230 Vgl. vorne, S. 64ff.

231 Gl. M. SCHWAPPACH, a.a.O.

durch das Persönlichkeitsrecht geschütztes Rechtsgut i.S. der Gütertheorie verletzen können.

Die grösste Gefährdung der Persönlichkeitsrechte geht dabei zweifellos von den personenbezogenen Daten aus, so dass an der Wirksamkeit einer an dieser Datennatur erfolgenden Anknüpfung zur Verwirklichung des Schutzes der Privatsphäre kein Zweifel bestehen kann.

Für sachbezogene Daten stellt sich die Problematik des Anknüpfungspunktes zur Schutzrealisierung anders. Sachbezogene Daten sind negativ als nicht personenbezogene Informationen abgrenzbar, beziehen sich somit nur auf eine Sache oder realen Vorgang. Die sachbezogenen Angaben vermögen weder im Kontext noch bei unterschiedlicher Interpretation oder einer Verbreitung die Persönlichkeitssphäre zu verletzen, da ihnen jeder personenbezogene Charakter fehlt; ihre vordergründige absolute Bezugslosigkeit zu Personen macht sie "ungefährlich" für die Privatsphäre i.S. der Sphärentheorie und der "persönliche Verhältnisse" als Rechtsgut i.S. der Gütertheorie.²³²

Die Beschränkung des Schutzes auf personenbezogene Daten engt die Geltendmachung des Persönlichkeitsrechts ein: Vor allem bei juristischen Personen verdeutlicht die Trennung von sach- und personenbezogenen Angaben, dass auch andere schützenswerte Rechtsgüter durch einen Missbrauch von sachbezogenen Informationen verletzt werden können, die letzten Endes in einer Beeinträchtigung in den persönlichen Verhältnissen resultieren können. So sind m.E. Forschungsprojekte und -ergebnisse, Planungen in Produktions-, Verkaufs- und Finanzbereich, Informationssysteme, aber auch statistische Angaben und Marktforschungsdaten ebenso schützenswert. Ihre Preisgabe kann eine Verletzung des geschäftlichen Geheimbereichs zur Folge haben, obwohl die Daten ihrer Natur nach sachbezogen sind. "Die Schutz und Sicherungs-

232 Sphärentheorie: vgl. GROSSEN; Einzelperson, S. 369; HOTZ, S. 69ff.; JAEGGI, S. 266a ff.; HUBMANN, S. 269ff.; SCHUCAN, S. 16ff.; ferner BGE 97 II 100, E. 3.
Gütertheorie: vgl. BUCHER, S. 88ff.; EGGER, Art. 28 N 24; HOTZ, S. 39ff.

problematisch für solche Informationen sind im Unternehmen genauso gegeben wie für personenbezogene Daten.^{233 234}

Ich halte es aber nicht für angemessen, grundsätzlich alle Daten, gleichgültig, ob personen- oder sachbezogenen Charakters, zu schützen, - obwohl es im Interesse der Rechtssicherheit als nützlich erscheinen könnte - da dies für Handel und Wirtschaft, Industrie, Forschung und Verwaltung eine unverhältnismässige und rechtspolitisch nicht vertretbare Einschränkung der Datenverarbeitung darstellen würde, die letztlich in einem Versiegen des Datenverkehrs schlechthin enden könnte. Trotzdem sollte m.E. ein Weg gefunden werden, in bestimmten Ausnahmefällen sachbezogenen Daten einen Schutz zuzuerkennen. Als Lösungsmöglichkeit ist eine Ausdehnung des Schutzes auf sachbezogene Daten denkbar, die auch dem Schutz des Geschäftsgeheimnisses unterstehen. Mit einer solch eng umgrenzten Ausdehnung des Datenschutzes könnte m.E. nicht nur ein grösserer Bereich an schutzwürdigen Rechtsgütern abgedeckt, sondern gleichzeitig auch eine Beschränkung der Kontrollrechte (z.B. Einsichtsrecht) gegenüber juristischen Personen erreicht werden, d.h. juristische Personen dürften nicht zur Offenlegung von Informationen verpflichtet werden, die gleichzeitig Gegenstand des Geschäfts- und Unternehmensgeheimnisses darstellen.

Bei einem wirkungsvollen Datenschutz muss der Schutz der Persönlichkeitsrechte verwirklicht werden: Für eine Geltendmachung des Persönlichkeitsrechtes schlechthin muss es aber m.E. grundsätzlich unerheblich sein, ob die das Persönlichkeitsrecht bildenden persönlichen Güter, resp. Privat- und Geheimsphäre, sich aus personen- bzw. sachbezogenen Daten konstituieren, oder ob das Persönlichkeitsrecht durch personenbezogene oder sachbezogene Daten verletzt worden ist, wenn eine solche Verletzung objektiv feststeht.

Anders ausgedrückt: Eine durch sachbezogene Daten erfolgende Beeinträchtigung oder Verletzung der Persönlichkeit kann ebensowenig

233 NAGEL, Computer und Recht, S. 11.

234 Vgl. auch SCHOMERUS, Computer und Recht, S. 76.

gutgeheissen werden, wie ein durch personenbezogene Daten erfolgreicher Einbruch in die schützenswerte Privatsphäre.

V. Arten der internationalen Datenflüsse nach beteiligten Stellen²³⁵

Die Uebermittlung von Daten ins Ausland stellt im privaten Sektor nicht den Regelfall dar, sondern beruht meist auf besonderen wirtschaftlichen Notwendigkeiten oder auf einem Bekanntgabebeerfordernis, das ausländische Behörden privaten Gesellschaften stellen; aufgrund völkerrechtlicher Vereinbarungen existiert im öffentlichen Bereich vereinzelt ein Datenverkehr zwischen nationalen Behörden zweier Länder.

1. Datenflüsse zwischen nationalen Gesellschaften und nationalen, rechtlich unselbständigen Niederlassungen im Ausland

Nationale Unternehmen entfalten im Ausland ihre Tätigkeit, ohne dass dazu spezielle Organisationsformen notwendig sind (z.B. Baustellen im Ausland). Die Gesellschaftsform der im Ausland liegenden unselbständigen Niederlassung richtet sich meistens nach dem Recht des ausländischen Staates. Zwischen diesen Stellen kann ein Austausch sach- und personenbezogener Daten stattfinden.

2. Datenflüsse zwischen nationalen und ausländischen Gesellschaften

Hier handelt es sich um einen Datenaustausch zwischen nationalen und ausländischen, rechtlich selbständigen Stellen. Die häufigsten Erscheinungsformen weisen die multinationalen Gesellschaften auf, die eine Datenkommunikation unter den im Verbund stehenden Unternehmen betreiben.²³⁶ Ferner findet ein Datenverkehr zwischen durch Interessen oder Verträge miteinander verbundenen Gesellschaften statt.²³⁷

235 Die Einteilung folgt weitgehend derjenigen SCHWAPPACH's (DS+DS 1/78, S. 21).

236 Vgl. IBM, vorne, S. 73ff.

Der Datenaustausch zwischen Produktionsfirmen und Zulieferunternehmen bzw. Verteilgesellschaften im Ausland, ist im europäischen Raum relativ häufig und betrifft meistens sachbezogene Daten. Auf privater Ebene wirkt das Konkurrenzprinzip als hemmender Faktor für eine Weitergabe von personen- oder sachbezogenen Daten an die in der gleichen Branche tätigen Unternehmen. Die Mehrheit der exportierten bzw. importierten Daten ist sachbezogener Natur, wobei aber bei verbundenen Unternehmen der Fertigungsindustrie und Chemie sowie im Finanz- und Kreditbereich personenbezogene Angaben ausgetauscht werden.

3. Datenflüsse zwischen nationalen Gesellschaften und öffentlichen Stellen im Ausland

Die Uebermittlung von Daten beruht in diesem Falle vornehmlich auf gesetzlichen Bestimmungen des betreffenden ausländischen Staates. Diese Vorschriften erstrecken sich sowohl auf sach- wie personenbezogene Daten, die in Fiskalinformationen, Zolldeklarationen, Angaben über Auslandsinvestitionen zur Devisenkontrolle resultieren können. Daten zu natürlichen Personen werden i.d.R. nur zwecks Arbeitserlaubnis, Aufenthaltsgenehmigungen und fiskalischen Gründen übermittelt, wenn die Gesellschaften die Formalitäten für ihr Personal mit der ausländischen Behörde abwickeln.

4. Datenflüsse zwischen nationalen Behörden des öffentlichen Rechts und öffentlich-rechtlichen Stellen im Ausland

Grundlage eines solchen Datenaustausches bilden normalerweise völkerrechtliche Verträge i.S. von Konventionen oder zwischenstaatlichen Verträgen, die auf verschiedenen Behördengebieten denkbar sind. Nebst der Zusammenarbeit von nationalen Behörden in administrativen Belangen, existiert auch ein intensiver Datenaustausch bei militärischen Bündnissen zwischen Nationen. Als bekanntestes Beispiel

eines internationalen Datenverkehrs kann die Zusammenarbeit der Interpol²³⁸ und nationalen Polizeistellen dienen, ferner existieren zwischen den einzelnen Staaten eine Vielzahl von bi- oder multilateralen Verträgen (vgl. z.B. diverse Rechtshilfeabkommen). Amerikanische und kanadische Steuerbehörden tauschen Daten über die Einkommen und Vermögen ihrer Staatsbürger, die im andern Lande wohnen, aus; ein steuerbezogener Informationsaustausch besteht für gewisse Fälle auch unter den EG-Staaten. Zwischen Kanada und der BRD, Italien und der BRD existieren Vereinbarungen zum Austausch von Sozialversicherungsangaben.²³⁹ Auf militärischem Gebiet ist die Radarwarnung in Kanada mit dem amerikanischen Flugabwehrzentrum verbunden, daneben gibt es Datenflüsse logistischer Natur, die auch personenbezogene Daten enthalten.²⁴⁰

Innerhalb der Behörden ist der Anteil der ausgetauschten personenbezogenen Informationen grösser (absolut gesehen ist er kleiner), als im privaten Bereich, so dass eine Kontrolle des Datenexportes und -importes auch im öffentlichen Bereich angemessen erscheint.

5. Datenverarbeitung im Ausland im Auftrag eines nationalen Unternehmens oder einer öffentlichen nationalen Stelle

Hier ist an das Beispiel von EPCS²⁴¹ und anderer Service-Rechenzentren zu denken: Ein nationales Unternehmen übermittelt an ein ausländisches Rechenzentrum Daten, um sie dort verarbeiten zu lassen, eventuell um sie mit andern verbundenen Gesellschaften²⁴²

238 Vgl. vorne, S. 109ff.

239 So werden im Bereich der Sozialversicherung von deutschen Behördenstellen Bänder mit Daten zu in Italien lebenden deutschen Rentnern von Deutschland nach Italien gesandt und im italienischen Ministerium in den Computer eingelesen, damit die Rente in Italien durch die entsprechende Behörde den Empfangsberechtigten ausbezahlt werden kann.

240 Vgl. CAROLL, OECD-Informatics Studies 10, S. 202f.

241 Vgl. vorne, S. 81ff.

242 SCHWAPPACH (a.a.O.) hält die Zahl der verbundenen multinationalen Unternehmen, die Datenverarbeitung durch ein ebenfalls zum Verbund gehörendes zentrales Rechenzentrum betreiben oder die Datenverarbeitung überhaupt ausgliedern, für minimal, weil Kostenüberlegungen und Selbständigkeitsstreben von Konzerntöchtern solchen Trends entgegenwirken.

zu konsolidieren. Diese Möglichkeit der Auftragsdatenverarbeitung findet in der Praxis vor allem bei mittleren und kleinen, z.T. auch grösseren Gesellschaften mit internationaler Tätigkeit Anwendung. Sprachliche Barrieren können eine hemmende Rolle im Gebrauch von ausländischen Service-Rechenzentren bilden; viele der standardisierten Applikationen erfordern allerdings eine Befehls-, d.h. Kommunikationssprache, die programmgebunden ist (meistens englisch) und keinen Einfluss auf den Datenbestand als solchen hat. Die Ausgabe der Daten erfolgt oft in englischem Kontext, der aber für das datenverarbeitende Personal tägliches Arbeitsinstrument bedeutet. Sehr selten wird eine öffentlich-rechtliche Stelle die zur Erfüllung ihrer Aufgabe notwendige Datenverarbeitung einem ausländischen Rechenzentrum übertragen, sondern lokalen oder zumindest nationalen Verarbeitungszentren übergeben. Die Datenverarbeitung im Ausland im Auftrag von nationalen Stellen des privaten und öffentlichen Sektors wird im Rahmen der mit Euronet-Diane angebotenen Datenbanken verstärkt anwachsen. Für die Zukunft ist demnach zu erwarten, dass öffentliche wie private Stellen mit ausländischen Rechenzentren Verträge auf Datenbankabfragen abschliessen, so dass in vermehrter Masse sachbezogene und z.T. personenbezogene Angaben zwischen ausländischen Rechenzentren und privaten oder öffentlichen nationalen Stellen fliessen.

6. Datenflüsse innerhalb von internationalen Organisationen

Auch innerhalb internationaler Organisationen ²⁴³ gibt es ein bedeutendes Volumen an grenzüberschreitendem Informationsfluss, bedingt durch die Zusammenarbeit der geographisch verschiedenen Sitze dieser Organisationen, aber auch durch die Kooperation mit den nationalen Stellen.

²⁴³ Z.B. WMO (OCDE, Utilisation des Réseaux, S. 172ff.), CERN (a.a.O., S. 178ff.), Internationale Atomenergiebehörde, WHO (FREESE, Data Flow, S. 28), u.a.

§ 9 VERGLEICHENDER UEBERBLICK GESETZLICHER REGELUNGEN

I. Umfang

Die folgenden Ausführungen beschreiben in einer synoptischen Zusammenstellung verschiedene, für den grenzüberschreitenden Datenverkehr wichtige Aspekte einiger bestehenden Datenschutzgesetze und Entwürfe; sie sollen Unterschiede, aber auch gewisse Aehnlichkeiten oder Analogien der nationalen Rechtserlasse aufzeigen, um einen umfassenden Ueberblick der nationalen Regelungen im Hinblick auf eine Koordination des Datenschutzrechtes auf internationaler wie nationaler¹ Ebene zu verschaffen.

1. Allgemeine Grundzüge nationaler Gesetze

Im folgenden beschränke ich mich hauptsächlich auf die rechtlichen Grundsätze und Prinzipien der Gesetze, deren Anwendungs-, Schutz- und Geltungsbereiche sowie auf die bemerkenswerten Eigenarten der einzelnen Erlasse.

A. Anwendungsbereich²

Der Anwendungsbereich eines jeden Datenschutzgesetzes oder entsprechender Erlasse ist abhängig von der rechtlichen Grundlage, auf welcher das betreffende Gesetz beruht. Der Anwendungsbereich ist vor allem im Rahmen des internationalen Datenverkehrs bedeutend, weil es weder für die nationalen, zwischenstaatlichen oder eine zu schaffende internationale rechtliche Regelung gleichgültig sein kann, ob die im Erlass bzw. Gesetz enthaltenen Vorschriften nur den privaten bzw. öffentlichen Bereich oder beide Sektoren betreffen.

1 De lege ferenda.

2 Unter Anwendungsbereich i.e.S. ist nur die für den öffentlichen und / oder privaten Sektor statuierte Anwendbarkeit eines Gesetzes zu verstehen, während der Anwendungsbereich i.w.S. den Anwendungsbereich eines Gesetzes schlechthin umfasst, d.h. dessen Anwendungsbereich i.e.S., Schutz- und sachlichen Geltungsbereich. In den nachfolgenden Ausführungen der Synopsis wird unter Anwendungsbereich immer der Begriff i.e.S. verstanden, wo dies nicht der Fall ist, ergibt sich aus dem Kontext.

Im öffentlichen Bereich treten oft unterschiedliche Lösungen zu Tage, die teils durch eine umfassende,³ teils durch eine eingeschränkte⁴ Kompetenz des Gesetzgebers begründet werden. Unter dem föderalistischen Prinzip sind nur die Bundesbehörden und die übrigen öffentlichen Stellen und Institutionen des Bundes an die Vorschriften des Bundes gebunden, während auf der staatlichen,⁵ Länder-,⁶ kantonalen⁷ oder kommunalen Stufe eine eigene Gesetzgebungskompetenz besteht. Diese verschiedenen Kompetenzebenen bedingen eine Vielzahl von stufenspezifischen Datenschutzgesetzen und Verordnungen im öffentlichen Bereich, die aber für die mit diesen Staaten bzw. Behörden kommunizierenden Personen nicht mehr transparent sind und Rechtsunsicherheit hervorzurufen vermögen, weil ihnen nicht mehr klar ist, nach welchen Normen ein grenzüberschreitender Datenverkehr von öffentlichen Stellen in föderalistisch strukturierten Staaten zu beurteilen ist.

Bei Betrachtung dieser unterschiedlichen nationalen Lösungen im öffentlichen Bereich wird deutlich, dass ein föderalistisches Prinzip, das mehreren Stufen eine Kompetenz zur rechtlichen Regelung des grenzüberschreitenden Datenverkehrs einräumt, nicht leicht praktikabel ist, weil an den einzelnen Daten nicht mehr erkennbar ist, auf welcher Stufe sie einzureihen sind.

Werden Daten einzeln weitergegeben, ist für den Empfänger oft noch unklarer, welche nationale Rechtsvorschrift zum grenzüberschreitenden Datenverkehr anzuwenden ist.

3 Nachfolgend auch zentralistisches Prinzip genannt.

4 Nachfolgend auch föderalistisches Prinzip genannt.

5 USA mit Datenschutzgesetzen und Erlassen in verschiedenen Bundesstaaten vgl. SMITH, Compilation of State & Federal Laws on Privacy, S. 2f./5ff.

6 BRD mit LDSG's in Hessen, Rheinland-Pfalz, Bayern, usw.

7 CH mit kantonalen und kommunalen Datenschutzverordnungen: vgl. PETITPIERRE, S. 87 ff.; SCHWEIZER, DS+DS 3/80, S. 155; ferner Computer und Privatsphäre, Computer und Recht, Band 6: Zusammenfassender Ueberblick über Stand der Entwicklung von Datenschutzvorschriften in Kantonen (S. 267ff.) und Uebersicht über Vorschriften betreffend Behandlung von Informationen und den Schutz von Daten im Bereich der kommunalen Verwaltung (S. 273ff.).

Als Ausweg könnte die rechtliche Gleichbehandlung aller Daten des öffentlichen Bereiches - unabhängig von der Kompetenzstufe - dienen, die in einem föderalistisch organisierten Lande eintreffen oder ausgeführt werden. Nur ein uniformer für alle Staaten möglichst einfacher Anknüpfungspunkt vermag sich im internationalen Datenverkehr als anwendbar und der Rechtssicherheit förderlich zu erweisen.⁸

Ungünstig kann sich - sowohl innerstaatlich als auch international - eine scharfe Grenzziehung zwischen den Bestimmungen (über den grenzüberschreitenden Datenverkehr) des öffentlichen und denen des privaten Bereiches auswirken.⁹ Innerstaatlich machen sich Unausgewogenheiten der Regelungen immer bemerkbar, wenn zwischen Datenverarbeitern, die dem Privatrecht, und Stellen, die dem öffentlichen Recht untergeordnet sind, Daten ausgetauscht werden; wenn dann Institutionen des privaten Sektors sogar öffentlich-rechtliche Aufgaben und Angelegenheiten anvertraut werden, erweist sich die Befolgung eines mit solchen Diskrepanzen behafteten Gesetzes als schwerfällig, wenn nicht sogar unpraktikabel.

Im internationalen Bereich kann sich eine unterschiedliche Regelung negativ auf den grenzüberschreitenden Datenverkehr auswirken, vor allem in denjenigen Fällen, bei welchen gewisse Handlungen und Verarbeitungsschritte in einem Land dem privaten Sektor zugeordnet werden, während sie im anderen Land in den Zuständigkeitsbereich des öffentlichen Rechts fallen.

Der Rechtssicherheit zuträglich ist eine möglichst grosse Ausgeglichenheit der Regelung der beiden Bereiche: dies bedeutet, dass für das öffentliche und private Recht von den gleichen Grundsätzen und Prinzipien ausgegangen und - gemäss der strukturellen Unterschieden dieser beiden Bereiche - die materiell- und formellrechtliche Ausgestaltung im öffentlichen Bereich nach dem Legalitätsprinzip und im privaten Bereich nach dem Vertrauensprinzip ausgerichtet werden soll-

8 Gilt auch für den nationalen Bereich; vgl. hinten, S. 333.

9 Vgl. HONDIUS, OECD-Informatics Studies 10, S. 216f.

te. Nicht auszuschliessen sind bereichsspezifische Ausnahmebestimmungen in beiden Sektoren, die aber von Interessenlobbies nicht zu einer Aushöhlung der allgemeinen für beide Bereiche geltenden Grundsätze missbraucht werden dürfen.

B. Bereich der geschützten Subjekte (Schutzbereich)

Einen hohen Stellenwert ¹⁰ nimmt auch die national unterschiedliche Ausgestaltung des Schutzbereiches ein, denn es kann für Datentransfers u.U. bedeutsam sein, ob in einem Lande nur Daten ¹¹ natürlicher oder auch juristischer Personen und Angaben von Personenvereinigungen ohne Rechtspersönlichkeit geschützt werden, vor allem angesichts der Tatsache, dass die beiden letzteren ein vergleichbares Schutzbedürfnis gegen Persönlichkeitsverletzungen aufweisen, wie natürliche Personen.

C. Sachlicher Geltungsbereich

Der Geltungsbereich, d.h. die Schutzwirkung für manuell und/oder nur automatisiert verarbeitete Daten, hat im grenzüberschreitenden Datenverkehr hervorstechende Bedeutung, weil sich in diesem Punkte die Wirksamkeit des Datenschutzes erweisen muss. Grosse Diskrepanzen im Geltungsbereich zwischen den einzelnen nationalen Gesetzen können, solange eine diesen Punkt klärende internationale Konvention fehlt, die Entstehung von "small data havens" ¹² unter den Ländern mit einer Datenschutzgesetzgebung verursachen. Gerade die Möglichkeit, innerhalb der Datenverarbeitung die verschiedenen Datenverarbeitungsschritte in mehreren Nationen durchführen zu lassen, muss die Forderung nach einem möglichst abgestimmten, globalen, sachlichen

10 Vgl. Instruktionen und Text einer Stellungnahme des amerikanischen State Departments für den Beobachter der USA beim Europarat-Meeting vom 16.-18. Oktober 1978 und die darin enthaltenen Erwägungen zu den "Legal Persons", in: TDR, Vol. 1, No. 7, S. 22ff.

11 In der Datenschutzgesetzgebung werden regelmässig nur personenbezogene Daten geschützt, damit die Persönlichkeitssphäre des Einzelnen gewährleistet werden kann.

12 Vgl. vorne, S. 44ff.

Geltungsbereich verstärken. Es kann zu Schranken im transnationalen Verkehr führen, wenn gewisse Datenverarbeitungsvorgänge oder vorbereitende Handlungen in einem Lande nicht vom Geltungsbereich des Gesetzes erfasst werden und dabei helfen, weitergehende Vorschriften anderer Nationen zu umgehen und ihrer Wirksamkeit zu berauben.

2. Rechtliche Regelung des grenzüberschreitenden Datenverkehrs in bestehenden Datenschutzgesetzen

Als Kernstück de vergleichenden Ueberblicks soll - nach den allgemeinen Grundzügen - die rechtliche Regelung des grenzüberschreitenden Datenverkehrs der verschiedenen nationalen Datenschutzgesetze untersucht und dabei Vorzüge und Nachteile offengelegt werden. Eine Beschreibung aller existierenden Datenschutzgesetze würde den Rahmen dieser Arbeit sprengen, so dass ich mich auf eine Auswahl der für die Schweiz wichtigsten und signifikantesten Erlasse beschränke.

II. Vergleich bestehender Datenschutzgesetze¹³

1. Bundesrepublik Deutschland: Bundesdatenschutzgesetz¹⁴

A. Allgemeines

Anwendungs-, Schutz- und Geltungsbereich sind international immer dann bedeutsam, wenn Daten von einem Land in das Rechtssystem eines andern (z.B. der BRD) treten und damit in den Geltungsbereich spezieller Datenschutzgesetze fallen.

a) Anwendungsbereich

Das BDSG schützt grundsätzlich die personenbezogenen Angaben¹⁵ (gleichgültig ob in- oder ausländischer Provenienz) in und aus Dateien während derer Verarbeitung bei allen privaten und öffentlichen Stellen.

Bei der Regelung für den öffentlichen Bereich gilt es zu präzisieren: § 7 BDSG normiert den Anwendungsbereich des Gesetzes für die Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen; dabei wird unterschieden zwischen Bundesbehörden¹⁶ und Landes- oder Kommunalbehörden.¹⁷ Für die Bundesbehörden gilt das BDSG ohne Einschränkung, für die Landes- oder Kommunalbehörden hingegen nur subsidiär,¹⁸ d.h. soweit in den Bundesländern beim Vollzug von Lan-

13 Vgl. auch BURKERT/ENGEL, DS+DS 3/80, S. 146ff.

14 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) vom 27. Januar 1977 (BGBl. I S. 201ff.).

15 Zu personenbezogenen Daten gehören nicht nur die persönlichen Daten, die der Persönlichkeitssphäre zugeordnete Angaben enthalten, sondern auch Angaben über sachliche Verhältnisse (vgl. HERGENHAHN, S. 25).

16 Behörden und sonstige öffentliche Stellen (z.B. Gerichte, parlamentarische Körperschaften usw.) des Bundes, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, Vereinigungen solcher Körperschaften, Anstalten und Stiftungen.

17 Behörden und sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände, juristische Personen des öffentlichen Rechts und deren Vereinigung, die der Aufsicht des Landes unterstehen.

18 Subsidiaritätsklausel des § 7 Abs.2 BDSG, auch Ländervorbehaltsklausel genannt (vgl. BERGMANN/MOEHRLE § 7 N 4.1) und § 45 BDSG (vgl. SENDLER, S. 81ff.).

desrecht der Datenschutz durch Landesdatenschutzgesetze (LDSG)¹⁹ und andere Spezialerlasse²⁰ i.S. von materiellen Vorschriften über den Datenschutz geregelt ist, ist das entsprechende Landesgesetz anwendbar: fehlen diesbezügliche Gesetze oder Erlasse in den Ländern, gilt das BDSG auch für die Landes- und Kommunalbehörden.

Dies ist ein typisches Beispiel einer föderalistischen Lösung im öffentlichen Sektor, die vor allem beim Austausch von Daten mit ausländischen privaten oder öffentlich-rechtlichen Institutionen zu Schwierigkeiten führen kann: eine Landes- bzw. Gemeindebehörde, die mit einer ausländischen Stelle Daten austauscht, hat zu prüfen, ob sie Landes- oder Bundesrecht vollzieht - je nach Rechtsnatur ist entweder das BDSG oder ein entsprechendes LDSG zuständig. Für die handelnde einheimische Behörde wird i.d.R. diese Unterscheidung wenig Schwierigkeiten bereiten, hingegen ist für die ausländische Stelle nicht klar erkennbar, in welchen Zuständigkeitsbereich (LDSG oder BDSG) die übermittelten Daten gelangen bzw. woher sie stammen und welchen Bestimmungen sie unterstehen. Diese Vielfalt an Gesetzen ist der Rechtssicherheit, der gerade im internationalen Bereich eine Schlüsselfunktion zukommt, abträglich. Im Interesse dieses Postulates sollte für den grenzüberschreitenden Datenverkehr eine einheitliche Regelung anwendbar sein, die von allen ausländischen Stellen als geltendes Recht betrachtet werden kann.

Der Anwendungsbereich des BDSG erstreckt sich auch auf den privaten Sektor, der nach dem Zweck der Verarbeitung in zwei Bereiche unterteilt ist:

- Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke²¹ und
- geschäftsmässige Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke.²²

19 Z.B. in Hessen, Bayern, Nordrhein-Westfalen.

20 Z.B. Baden-Württemberg: § 13 des Gesetzes über die Datenzentrale vom 17.11.1970.

21 3. Abschnitt des BDSG: §§ 22-30.

22 4. Abschnitt des BDSG: §§ 31-40.

Zum privaten Bereich gehören alle natürlichen und juristischen Personen oder Personenvereinigungen des Privatrechts, ohne Rücksicht auf deren Rechtsform, die Daten für eigene oder fremde Zwecke verarbeiten. Ausgenommen sind die Organisationen des Privatrechts, wenn sie Aufgaben der öffentlichen Verwaltung erfüllen: sie fallen diesfalls in den öffentlichen Bereich. Als Ausnahme im privaten Sektor des 3. Abschnittes können öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, genannt werden (z.B. öffentlich-rechtliche Versicherungen): sie sind den Gesellschaften des Privatrechts gleichgestellt. Ausserdem gelten die Normen des privaten Bereichs auch für dienst- und arbeitsrechtliche Verhältnisse öffentlicher Arbeitgeber, weil den Arbeitsverhältnisse sowohl im öffentlichen als auch im privaten Sektor die gleiche Behandlung bezüglich Datenschutz zuteil werden soll. Im 4. Abschnitt werden schliesslich die öffentlich-rechtlichen Unternehmen, die für fremde Zwecke Daten verarbeiten, den privaten gleichgestellt.

b) Schutzbereich

Aufgrund von § 1 Abs.1 schützt das BDSG nur die personenbezogenen Daten und präzisiert in § 2 Abs.1 diese Begriffsbestimmung, in dem Sinne, dass personenbezogene Daten als "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person" zu verstehen sind. Damit wird gleichzeitig der Schutzbereich *expressis verbis* auf die natürlichen Personen beschränkt. Diese Regelung ist als aussergewöhnlich zu betrachten, weil das Grundgesetz in Art. 19 Abs. 3 festlegt, dass die Grundrechte auch für inländische juristische Personen gelten, soweit sie auf diese wegen ihres besonderen Wesens und den fehlenden menschlichen Eigenschaften anwendbar sind. Diese Beschränkung auf natürliche Personen trägt m.E. der Tatsache zu wenig Rechnung, dass auch juristische Personen eine Art "Privatsphäre" besitzen können,²³ innerhalb derer

23 Die deutsche Lehre anerkennt grundsätzlich die Existenz der Privatsphäre von juristischen Personen: vgl. BERGMANN / MOEHRLE, § 2 N 1; DAMMANN/SIMITIS, § 2 N 2; SCHWAPPACH, BDSG, S. 20.

es eine Vielzahl schutzbedürftiger Daten gibt. Die Folge dieser Grenzziehung führt zu der grotesken Situation, dass die als Einzelkaufmann auftretende natürliche Person die Rechte des Betroffenen²⁴ auch in ihrem gewerblichen Bereich wahrnehmen kann, während juristischen Personen oder Personenvereinigungen solche Rechtsmittel nicht zustehen. Diese Rechtslage bevorzugt die als Einzelunternehmer tätigen natürlichen Personen, während der geschäftsführende Einmannaktionär einer Einmann-AG (um vergleichbare Grössen aufzuzeigen) als Geschäftsmann keine Rechte aus dem BDSG geltend machen kann. Diese Diskrepanz ist auf eine zu pauschale Abgrenzung der personenbezogenen Daten zurückzuführen: eine saubere Grenzziehung zwischen natürlichen und juristischen Personen müsste durch eine Trennung der verarbeiteten Daten nach ihrer Zugehörigkeit zum Individualbereich bzw. zum beruflichen oder gewerblichen Bereich ergänzt werden. Von einer Definition des Begriffs "geschäftliche Daten" wurde aber abgesehen, "weil Abgrenzungsschwierigkeiten befürchtet wurden".²⁵

c) Geltungsbereich

Der in § 2 Abs.2 festgelegte Geltungsbereich des BDSG bezieht sich nicht auf eine bestimmte Art der Datenverarbeitung und erfasst damit sowohl die manuellen als auch die automationsunterstützten Verfahren. Die dabei vorkommenden verschiedenen schutzrelevanten Phasen²⁶ werden ebenfalls begrifflich festgelegt und beinhalten auch

24 Z.B. Recht auf Auskunft: §§ 13; 26 Abs.2; 34 Abs.2 BDSG;
Berichtigungsrecht: §§ 14 Abs.1; 27 Abs.1; 35 Abs.1 BDSG;
Sperrungsrecht: §§ 14 Abs.2; 27 Abs.2; 35 Abs.2 BDSG;
Löschungsrecht: §§ 14 Abs.2; 27 Abs.2; 35 Abs.2 BDSG.

25 SCHWAPPACH, BDSG, S. 19

26 - Speicherung (i.S. von Aufbewahrung während einer gewissen Dauer) wird durch die Erfüllung der sie prägenden Handlungen des Erfassens, Aufnehmens und Aufbereitens definiert (ORDEMAN/SCHOMERUS, § 2 N 2.1, S. 41). Das Speichern muss auf einem Datenträger (Tape, Disk, Diskette, Lochkarte etc.) erfolgen.
- Uebermitteln der gespeicherten oder durch Verarbeitung neu entstandenen Daten an Dritte, vgl. hinten, S. 143.
- Verändern umfasst jede Form der inhaltlichen Umgestal-

die vorbereitenden Handlungen wie das Erfassen, Aufnehmen von Daten, (hingegen m.E. nicht die Datenbeschaffung, z.B. mittels Fragebogen). Eine entscheidende Rolle im Geltungsbereich des BDSG spielt der Dateibegriff: die Daten werden nach § 1 Abs.2 BDSG nur geschützt, wenn sie in oder aus einer Datei verarbeitet werden. Die Datei charakterisiert sich als Sammlung einer Mehrzahl von formal gleichartigen Daten in einem und nach bestimmten Merkmalen geordneten Aufbau, der sich nach andern Merkmalen umordnen oder auswerten lässt.²⁷ Damit werden nicht nur die durch automatisierte Verfahren erstellten Dateien, sondern auch die mit manuellen Mitteln geschaffenen Datensammlungen erfasst, falls sie die Charakteristika des Dateibegriffs nach § 2 Abs.3 Ziff.3 BDSG erfüllen. Der Dateibegriff weist allerdings noch Lücken auf, die vor allem dann zutage treten, wenn Sammlungen von Daten mit nur mit je einem Merkmal zur Diskussion stehen.²⁸ Diese gelten nach dem Wortlaut des Gesetzes nicht als Datei, obwohl sie in Wirklichkeit Dateiencharakter besitzen,²⁹ und genießen bei missbräuchlicher Datenverarbeitung somit keinen Gesetzesschutz.^{30 31} Ueber den Dateibegriff, dessen exakte Definition als eines der schwierigsten Probleme des Gesetzes gilt,³² gelingt es dem BDSG, die mit automationsunterstützten und manuellen Verfahren verarbeiteten personenbezogenen Daten zu schützen. Als weitere Voraussetzung wird im Zusammenhang mit dem Dateibegriff der Schutz für personenbezogene Daten nur wirksam, wenn sie "zum Zwecke ihrer weiteren Verwendung" gespei-

tung z.B. durch Ergänzung, Verknüpfung, partieller Löschung von Daten.

- Löschen bedeutet Unkenntlichmachung der Daten durch Vernichten, Ueberschreiben, Durchstreichen, so dass die Angaben unlesbar werden.

27 § 2 Abs.3 Ziff.3 BDSG.

28 Hierher sind z.B. personenbezogene Angaben, die im Zusammenhang mit der elektronischen Textverarbeitung gespeichert werden, zu zählen; WEISE, DS+DS 3/80, S. 139ff.

29 Nach dem 2. Tätigkeitsbericht d.B.f.D. (S. 60) sind in der Praxis alle Datensammlungen, die in automatisierten Verfahren verarbeitet werden grundsätzlich als Dateien zu betrachten.

30 BERGMANN/MOEHRLE, § 2 N 10.

31 LAICHER, DS+DS 3/78, S. 148ff.

32 SCHWAPPACH, BDSG, S. 22.

chert werden; wenn sie hingegen nur für einen bestimmten Zweck in den Computer aufgenommen, verarbeitet und wieder gelöscht werden,³³ entfällt das Erfordernis für die Schutzwirkung - ob dies genügt, wird die Zukunft aufgrund der praktischen Erfahrung zeigen.

B. Die rechtliche Regelung des grenzüberschreitenden Datenverkehrs

Im BDSG sind keine Bestimmungen enthalten, die sich ausdrücklich auf den grenzüberschreitenden Datenverkehr beziehen. Nach Ansicht verschiedener Autoren³⁴ lässt sich jedoch aus einer Vielzahl von Bestimmungen eine Beschränkung des Datenexportes herleiten.

Das Gesetz subsumiert den grenzüberschreitenden Datenverkehr unter die Datenverarbeitungsphase des Uebermittels i.S. von § 2 Abs. 2 Ziff. 2 BDSG. Definitionsgemäss ist für eine Uebermittlung ein "Dritter" i.S. von § 2 Abs. 3 Ziff. 2 BDSG als effektiver oder potentieller Empfänger erforderlich. Aus der Definition der "speichernden Stelle", die sich abgesehen vom Speichern auch durch Verändern, Uebermitteln und Löschen von Daten charakterisieren lässt,³⁵ folgt: "Wer nicht speichernde Stelle ist, muss Dritter sein, d.h. jede natürliche oder juristische Person des privaten oder öffentlichen Rechts ausserhalb der speichernden Stelle."³⁶ Dritte können somit als "rechtlich

33 SCHWAPPACH, BDSG, S. 20.

34 Vgl. AUERNHAMMER, BDSG, S. 9, 88 und 152;
SIMITIS/DAMMANN/MALLMANN/REH, BDSG, § 22 N 54ff.;
ORDEMANNSCHOMERUS, S. 130.

35 Als speichernde Stelle gelten aber auch diejenigen Personen und Institutionen, die selbst keine personenbezogenen Daten speichern, sondern durch andere speichern lassen. "Damit sind jene Fälle gemeint, in denen jemand seine personenbezogenen Daten durch ein externes Rechenzentrum 'ausser Haus' speichern und verarbeiten lässt." (ORDEMANNSCHOMERUS § 2 N 3.2, S. 44) In diesen Fällen verbleibt die Verantwortlichkeit für den Schutz der Daten bei der fachlich zuständigen Stelle, die die Herrschaft über die Daten ausübt - somit beim Auftraggeber, der damit berechtigterweise als speichernde Stelle genannt wird. Herr der Daten ist diejenige Person oder Stelle, die über deren Verwendungszweck entscheidet (GALLWAS/SCHNEIDER/SCHWAPPACH/SCHWEINICH/STEINBRINCK, BDSG § 2 N 31).

36 ORDEMANNSCHOMERUS, § 2 N 3.2, S. 44.

selbständige Stellen, die nicht bloss Hilfe zum Zweck der Datenverarbeitung leisten, sondern zu eigenen Zwecken Daten verarbeiten", umschrieben werden. Rechtlich unselbständige Betriebe oder Abteilungen, deren Aufgabe es ist für das eine einheitliche juristische Person bildende Unternehmen als Erfüllungsgehilfe die Datenverarbeitung durchzuführen, sind keine Dritten;³⁷ eine Datenverschiebung zwischen zwei Abteilungen ist somit keine Uebermittlung i.S. von § 2 Abs. 2 Ziff. 2 BDSG.

Bei verbundenen Unternehmen (Konzernen) sind die rechtlich verselbständigten Einheiten untereinander und in ihrer Beziehung zur Muttergesellschaft Dritte: bei Datenverschiebungen erfolgt somit eine Uebermittlung i.S. des Gesetzes. Eine Ausnahme bildet der Fall, wo Tochtergesellschaften untereinander oder die Muttergesellschaft im Auftrag für eine oder mehrere Töchter Daten verarbeitet, ohne ein eigenes Interesse an den Daten zu haben.³⁸ Diejenigen Personen und Stellen, die Daten im Auftrag anderer verarbeiten, gehören nicht zum Kreis der Dritten i.S. von § 2 Abs. 3 Ziff. 2.³⁹ Diese Ausnahmeregelung findet aber nur im Inland, d.h. innerhalb des Geltungsbereiches des BDSG Anwendung, so dass im Ausland befindliche Rechenzentren, welche Daten im Auftrage Dritter verarbeiten, als Dritte zu qualifizieren sind, weil sie nicht mehr im Wirkungsbereich des BDSG liegen. Für die Datenverarbeitung, mit der ein ausländisches Rechenzentrum beauftragt wird, ist somit der normale Tatbestand des Uebermittlens erfüllt: Für ihn sind die im Gesetz genannten Voraussetzungen erforderlich.

Weil öffentliche und private Datenverarbeitungsstellen im Ausland nicht in den Geltungsbereich des BDSG fallen, sind sie als Dritte zu qualifizieren und unterliegen den Zulässigkeitsvoraussetzungen der Datenübermittlung nach § 11 BDSG für den öffentlichen Bereich⁴⁰ und nach § 24 BDSG für den privaten Sektor.

37 SCHOMERUS, DS+DS 1/80, S. 7.

38 Vgl. SCHWAPPACH, BDSG, § 2 N 8, S. 21.

39 Vgl. Ausnahmefall der speichernden Stelle, Anm. 35, vorne, S. 143.

40 BERGMANN/MOEHRLE, § 11 N 4+5.

a) Im öffentlichen Bereich: § 11 BDSG

Satz 3 regelt die Uebermittlung personenbezogener Daten an öffentliche,⁴¹ private und internationale⁴² Stellen im Ausland.⁴³ Die Formulierung des Satzes kennzeichnet aber gleichzeitig die Subsidiarität dieser Bestimmung gegenüber speziellen, für den grenzüberschreitenden Datenverkehr bestehenden Gesetzen, Landesvereinbarungen⁴⁴ oder völkerrechtlichen Verträgen, die dem BDSG vorgehen; diese besonderen Erlasse oder Vereinbarungen dürfen allerdings nicht im Widerspruch zu den Grundgedanken des Datenschutzes stehen, "da diese Verfassungsrang haben (Art. 1 und 2 GG)."⁴⁵ Bei einem Fehlen solcher abweichenden Regelungen findet das BDSG Anwendung, einschliesslich der in Satz 1 und 2 (§ 11) aufgestellten Voraussetzungen für Datenübermittlung an Stellen ausserhalb des öffentlichen Bereichs.

Als Voraussetzungen für eine zulässige Uebermittlung kann einerseits vorgebracht werden, dass die zu erfüllende Aufgabe der Behörde eine solche Uebermittlung erfordert, und andererseits, dass der Empfänger im Ausland ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft machen kann und mit der Uebermittlung keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden. In concreto bedeutet dies, dass ausländische private, öffentliche oder internationale Stellen die deutschen Behörden um Uebermittlung der Daten ersuchen müssen, wobei deren Bewilligung von den genannten Voraussetzungen⁴⁶ abhängig ist. Die übermittelnde deutsche Behördenstelle hat bei jedem Gesuch das berechtigte Interesse der ausländischen Stelle zu prüfen und abzuwägen, ob schutzwürdige Belange des Betroffenen

41 Ausländische Behörden werden nicht wie inländische Behördenstellen nach § 10 BDSG behandelt, sondern wie private Empfänger im Inland (vgl. BERGMANN/MOEHRLE, § 11 N 5).

42 Auch zwischenstaatliche und überstaatliche.

43 ORDEMANN/SCHOMERUS, BDSG § 11 N 3, S. 73.

44 Subsidiarität des BDSG auch gegenüber Vereinbarungen der Bundesländer mit ausländischen Stellen.

45 SCHWAPPACH, BDSG, S. 32.

46 Auch völkerrechtliche Vereinbarungen (ORDEMANN/SCHOMERUS, OeVD 6/77, S. 4; KASPERS, DS+DS 2/80, S. 83).

mit einer Uebermittlung beeinträchtigt werden könnten; eine negative Beantwortung der letzteren Voraussetzung wird vor allem dann anzunehmen sein, wenn im Destinationsland keine oder nur ungenügende Datenschutzregelungen gelten. Sollten die schutzwürdigen Belange einer Weitergabe entgegenstehen, kann nur noch die Zustimmung der betroffenen Person eine Weitergabe der Daten ins Ausland ermöglichen.⁴⁷ Laut Satz 2 muss die um Uebermittlung ersuchte Behördenstelle für personenbezogene Daten, die einem Berufs- oder Amtsgeheimnis unterliegt, zusätzlich prüfen, ob auch den Destinatären gegenüber "die besonderen Voraussetzungen für eine Ausnahme von der grundsätzlichen Verschwiegenheitsverpflichtung bestehen."⁴⁸ Diese sehr restriktive Regelung für eine Weitergabe basiert auf der Ueberlegung, dass die öffentliche Hand aufgrund gesetzlicher Bestimmungen vom einzelnen Individuum in grösserem Ausmasse personenbezogene Informationen erfragen und verlangen kann als private Stellen. Ein besonders sorgfältiger Umgang mit diesen personenbezogenen Daten, vor allem gegenüber privaten und ausländischen Stellen, scheint daher im Interesse eines jeden Individuums zu liegen.

b) Im privaten Bereich: § 24 BDSG

Die materiellen Regelungen des BDSG im privatrechtlichen Bereich sind abschliessend. § 24 normiert die Uebermittlung (eine der vier vom Gesetz aufgezählten Phasen der Datenverarbeitung) personenbezogener Daten an Dritte. Als Dritter bzw. Empfänger von Daten können "alle natürlichen Personen, alle Behörden und sonstigen öffentlichen Stellen deutschen oder fremden Rechts, alle juristischen Personen, Gesellschaften und anderen Personenvereinigungen des privaten Rechts, welcher Rechtsordnung auch immer sie angehören",⁴⁹ in Frage kommen. In diesem Paragraphen wird somit die nationale als auch internationale Uebermittlung personenbezogener Daten zwischen speichernden Stellen geregelt, so dass § 24 BDSG auch für den innerhalb des privaten

47 ORDEMANN/SCHOMERUS, a.a.O.

48 SCHEDL, BDSG, S. 46/47.

49 AUERNHAMMER, BDSG § 24 N 5, S. 152.

Bereiches erfolgenden Export von in der BRD gespeicherten und geschützten Daten ins Ausland anwendbar ist.

Die Uebermittlung geschützter Daten ist aufgrund von zwei alternativ existierenden Voraussetzungen zulässig, einerseits, wenn ein Vertragsverhältnis zwischen dem Betroffenen und der den grenzüberschreitenden Datenverkehr fordernden Stelle besteht, oder andererseits, wenn eine Uebermittlung personenbezogener Daten zur Wahrung berechtigter Interessen der Übermittelnden (absendenden und speichernden) Stelle, eines Dritten bzw. der Allgemeinheit notwendig ist und dabei in keiner Weise schutzwürdige Belange des Betroffenen beeinträchtigt werden. Die Abwägung des berechtigten Interesses mit der potentiellen Beeinträchtigung in den schutzwürdigen Belangen wird von der Übermittelnden Stelle vorgenommen, die sowohl für die Richtigkeit der Weitergabe haftet als auch die Verantwortung für allfällige Schadenersatzklagen trägt.⁵⁰

Bei der Beurteilung des berechtigten Interesses, das die speichernde Stelle, ein Dritter oder die Allgemeinheit äussern kann, ist ein sehr weiter Spielraum des Ermessens möglich, der nach Auffassung der Doktrin zum BDSG auch präventive Massnahmen abdeckt, wie z.B. die Uebermittlung von Daten durch Kreditinstitute oder Wirtschaftsbetriebe an Schutzorganisationen.^{51 52} Die Abwägung einer Beeinträchtigung schutzwürdiger Belange erfordert eine in jedem Einzelfalle zu vollziehende Interessenabwägung nach dem Verhältnismässigkeitsprinzip.

Als Ausnahmeregelung ist noch aufzuführen, dass personenbezogene Daten, die einem Berufs- und Amtsgeheimnis unterliegen und "im Rahmen der Verschwiegenheitspflicht" legal "an die nicht unter dieser Verschwiegenheitspflicht stehende speichernde Stelle übermittelt worden

50 SCHEDL, BDSG, S. 81.

51 SCHEDL, a.a.O.

52 Beschreibung eines Beispiels, vgl. DER SPIEGEL, 33. Jg., Nr.1 vom 1.1.1979; ferner VOSS, S. 183ff.

sind, von dieser nicht mehr übermittelt" ⁵³ werden dürfen. Dies ist eine logische Konsequenz, die aus dem Berufs- und Amtsgeheimnis folgt und dessen Wirksamkeit nicht durch ein wiederholtes Uebermitteln aushöhlen soll.

Bei allen Tatbeständen sanktioniert aber eine schriftliche Einwilligung des Betroffenen die fehlenden Voraussetzungen der Uebermittlung. ⁵⁴

Bei widerrechtlicher Uebermittlung wird die Speicherung der weitergegebenen Daten unzulässig und muss rückgängig gemacht werden, z.B. durch Löschung des übermittelten Datenbestandes und der daraus erzielten Umformung anderer Dateien. Dabei ist unerheblich, ob der Empfänger der Daten eine öffentliche, private oder supranationale Stelle im In- oder Ausland ist. Der unbefugt Uebermittelnde ⁵⁵ ist für den Schaden verantwortlich und nach § 41 Abs.1 Ziff.1 und Abs.2 BDSG strafbar.

In Abs. 2 von § 24 BDSG ist für sog. "freie Daten" eine Sonderregelung im privaten Bereich ⁵⁶ erlassen worden, die darin besteht, dass für deren alleinige Uebermittlung keine speziellen Voraussetzungen nach Abs. 1 notwendig sind. Die Uebermittlung hat jedoch listenmässig, d.h. in grossem Umfang zu erfolgen und ist auf die aufgezählten Daten beschränkt (Name; Titel, akademische Grade; Geburtsdatum; Beruf, Branchen- oder Geschäftsbezeichnung; Anschrift und Rufnummer). Es darf aber kein Grund zur Annahme bestehen, dass die "massenweise" Uebermittlung schutzwürdige Belange eines Betroffenen beeinträchtigen könnte.

53 AUERNHAMMER, BDSG, § 24 N 10, S. 153f.

54 KASPERS, (DS+DS 2/80, S. 83) bezweifelt, dass der Betroffene in der Lage sei, als Nichtexperte in Sachen Datenschutz die Verletzung zu konstatieren und in Abhängigkeit von seinem Befund eine Einwilligung auszusprechen bzw. zu widerrufen.

55 Z.B. wegen fehlender Zulässigkeitsvoraussetzung, mangelnder Einwilligung, etc.

56 Im öffentlichen Bereich dürfen Behörden diese Daten nur gemäss § 11 BDSG an Dritte weitergeben: im öffentlichen Bereich wurde bei der Datenübermittlung somit nicht eine spezielle Kategorie personenbezogener Daten geschaffen.

Ebenfalls unter die Bestimmung des § 24 BDSG sind die Fälle der Datenverarbeitung im Auftrag einzuordnen, bei denen sich das beauftragte Rechenzentrum im Ausland befindet,⁵⁷ da sich dieses Rechenzentrum als Dritter i.S. von § 2 Abs.3 Ziff.2 BDSG qualifiziert.^{58 59}

In allen Fällen, in denen die Erlaubnistatbestände des § 3 Ziff. 1 i.V. mit den §§ 11 und 24 BDSG zur Uebermittlung von personenbezogenen Daten nicht anwendbar sind, ist laut § 3 BDSG die Einwilligung des Betroffenen notwendig.

C. Folgerung

Die Regelung des grenzüberschreitenden Datenverkehrs im BDSG ist schwerfällig und wenig transparent, weil spezifisch auf den Datenexport bzw. -import zugeschnittene Bestimmungen fehlen.

a) Datenausfuhr

SCHWAPPACH bedauert, dass § 11 BDSG, der die Datenübermittlung öffentlicher Stellen an Behörden, sonstige öffentliche Institutionen und private Stellen oder internationale Gremien im Ausland regelt, an einem versteckten Platz im Gesetz steht, da der Datenaustausch in diesem Bereich in nächster Zukunft zunehmend Bedeutung erlangen wird (z.B. im Rahmen der EG).⁶⁰ Diese Vermutung wird vom Verfasser unterstützt und dabei auch hervorgehoben, dass vor allem im öffentlichen Bereich eine klare Aussage über Zulässigkeit und Voraussetzungen der Datenausfuhr an ausländische Stellen des privaten und öffentlichen Sektors erlassen werden müsste, damit dem Individuum Schutz der Daten zuteil wird, die die öffentliche Hand kraft ihrer obrigkeitlichen Befugnisse in grossem Umfang zu sammeln imstande ist. § 11 BDSG ist für eine extensive Datenausfuhr, wie sie in den nächsten Jahren einsetzen

57 Vgl. auch SCHWAPPACH, DS+DS 1/78, S. 24.

58 Vgl. vorne S. 143f.

59 HERGENHAHN, S. 29.

60 SCHWAPPACH, BDSG, S. 32.

wird, wenig tauglich, Restriktionen und abgestufte Regelungen beim Export vorzunehmen. Vor allem wird die Subsidiarität des BDSG es den Betroffenen, aber auch den ausländischen Empfängern von Daten erschweren, den gesetzlichen Anknüpfungspunkt zu eruieren und ausserdem bei Amtshilfe die zuständige Behörde ausfindig zu machen.

Noch weit mehr als SCHWAPPACH dies für den öffentlichen Bereich tut, muss das Fehlen von spezifischen Bestimmungen zur Datenausfuhr im privaten Bereich bedauert werden, weil hier einerseits der Umfang der Datenein- und -ausfuhr grösser ist als im Verkehr von Behörden und andererseits der Stellenwert des grenzüberschreitenden Datenverkehrs zur Zeit der Gesetzgebung bereits bekannt war. Die Aufstellung eines einheitlichen Uebermittlungsbegriffes für den nationalen wie internationalen Bereich ist grundsätzlich zu begrüssen, doch weist die Bestimmung wegen der Uniformität ihrer Gültigkeit für nationale und internationale Datenflüsse Schwachstellen auf, die einer differenzierten Handhabung des grenzüberschreitenden Verkehrs kaum Möglichkeiten bieten. Die gegenüber dem öffentlichen Bereich weniger restriktive Handhabung der Uebermittlung ist begrüssenswert, weil ein grosser Teil der geschützten Daten entweder auf einer innergesellschaftlichen Grundlage oder auf vertraglicher bzw. vertragsähnlicher Vertrauensbasis exportiert wird.⁶²

Die Beurteilung der Normen zur Datenausfuhr müssen nicht nur innerstaatlich ihre Funktionsfähigkeit und Praktikabilität unter Beweis stellen, sondern auch einer kritischen Betrachtung durch die ausländischen Empfänger von Daten standhalten, vor allem bei einer Abwägung schutzwürdiger Belange des Betroffenen. Für eine Analyse dieser Frage wären jedoch spezifische, den internationalen Datenverkehr betreffende Bestimmungen bzw. deren Schutzvermögen ausschlaggebend, wenn es um eine Ausschaltung von lecken Stellen, d.h. einer Vermeidung von "data havens" geht. In diesem Sinne bezweifelt STAD-

61 D.h. zwischen unter- und übergeordneten Gesellschaften oder stufengleichen Unternehmen.

62 Vgl. auch SCHWAPPACH, DS+DS 1/78, S. 21ff.

LER ⁶³ eine positive Beurteilung der §§ 11 und 24 BDSG hinsichtlich einer ausreichenden Verhinderung von Datenleckstellen beim grenzüberschreitenden Datenverkehr unter Staaten, die in einer internationalen Datenschutzkonvention verbunden sein könnten und sich untereinander zu einem freien Datenaustausch bekennen würden.

Im Sinne einer Generalklausel für die Beurteilung der Zulässigkeit der Datenausfuhr wird in den §§ 11 und 24 BDSG letztlich auf eine potentielle Beeinträchtigung schutzwürdiger Belange des Betroffenen abgestellt. Diese bedingt bei jedem Export eine individuelle Beurteilung der Interessenlage. "Die Beurteilung, wann schutzwürdige Belange des Betroffenen vorliegen, ist allein nach Datenschutzgesichtspunkten im Hinblick auf das geschützte Rechtsgut 'Persönlichkeit' vorzunehmen."⁶⁴ Eine positive Beurteilung der schutzwürdigen Belange als Behaftung wird demgemäss weitgehend durch die Gewährleistung des Datenschutzes durch die Gesetze im Destinationsland bestimmt. Die Entscheidung zum Datenexport ist der eigenen Verantwortlichkeit jeder datenverarbeitenden Stelle anheimgestellt. Diese Eigenverantwortlichkeit kann im Einzelfall profunde Rechtskenntnisse des Entscheidungsträgers voraussetzen. Es ist jedoch fraglich, ob diese Entscheidungsgremien den Anforderungen gewachsen sind, wenn es um derart subtile Interessenabwägungen geht. Ueberdies ist einer solchen Regelung die Gefahr inhärent, dass eine übermässige Vorsicht des Entscheidungsträgers sich negativ auf den Datenaustausch auswirken kann. M.E. würden sich periodisch, vom Bundesbeauftragten für Datenschutz publizierte Informationen ⁶⁵ zur Beurteilung der in andern Staaten existierenden Beeinträchtigung schutzwürdiger Belange positiv auswirken, eine Abhängigkeit der Freigabe des Datenexportes von individuellen Zufälligkeiten verhindern sowie den am internationalen Datenverkehr Beteiligten grössere Rechtssicherheit bieten.

63 STADLER, DS+DS 3/79, S. 172.

64 SCHWAPPACH, BDSG, S. 32.

65 Eventuell wäre sogar eine spezielle Auskunft und Beratungsstelle denkbar und hilfreich.

Der folgende von SCHWAPPACH ⁶⁶ aufgeführte Ausnahmefall kann im BDSG ebenfalls als Schwachstelle gewertet werden, wenn es um die Vermeidung von "data havens" geht: Beim Export personenbezogener Daten einer unselbständigen Niederlassung an die Hauptgesellschaft im Ausland ist § 24 BDSG nicht anwendbar, weil die rechtlich unselbständige Betriebsstätte im Inland nicht als Dritter i.S. von § 2 Abs. 3 Ziff. 2 BDSG zu qualifizieren ist. "Gleichwohl ist der Betroffene nicht ungeschützt, da die unselbständige Stelle die Zulässigkeitsvoraussetzungen bei der Speicherung zu beachten hat."⁶⁷ Die Zulässigkeitsvoraussetzungen statuieren hierbei, dass Daten nur im Rahmen der Zweckbestimmung des Vertrages oder vertragsähnlicher Vertrauensverhältnisse und in dem dazu notwendigen Umfang gespeichert werden dürfen; alternativ ist eine Speicherung zulässig, wenn das berechtigte Interesse an der Speicherung dargelegt ist und die Daten als erforderliche Hilfsmittel zur Erfüllung des Geschäftszweckes dienen, ohne dass dabei konkrete Gründe zur Annahme einer Beeinträchtigung in den schutzwürdigen Belangen des Betroffenen bestehen. Eine objektive Beurteilung dieser beiden alternativen Zulässigkeitsvoraussetzungen kann am Abhängigkeitsverhältnis der speichernden Stelle im Inland von der Hauptgesellschaft im Ausland scheitern. Keine Gesellschaft, die Schwachstellen im Gesetz sucht, wird zugeben, dass mit einer Speicherung und gesellschaftsinternen Verschiebung der Daten (die nicht als Uebermittlung qualifiziert werden kann) schutzwürdige Belange des Betroffenen beeinträchtigt sein könnten; sie wird vielmehr die Daten durch die Betriebsstätte in der BRD sammeln, speichern und hierauf an den Hauptsitz im Ausland weitergeben, womit sie sie den für den Datenexport festgelegten Bestimmungen des BDSG entzieht. Durch die Errichtung unselbständiger datenspeichernder Stellen in der BRD durch Gesellschaften mit Sitz im Ausland könnte somit eine Umgehungsmöglichkeit der Schutzbestimmungen des BDSG geschaffen werden.

⁶⁶ SCHWAPPACH, DS+DS 1/78, S. 24.

⁶⁷ Id; a.a.O.

Kontroverse Standpunkte ⁶⁸ existieren auch bei der rechtlichen Qualifikation des Datenverkehrs zwischen einer im Inland (BRD) befindlichen Hauptniederlassung und einer im Ausland lokalisierten unselbständigen Zweigstelle. Wie vorne ausgeführt, ist der Datenverkehr zwischen der Zentrale und den unselbständigen Zweigstellen innerhalb der BRD nicht als Uebermittlung i.S. des BDSG zu qualifizieren.⁷⁰ Diese Beurteilung folgt aus der Betrachtungsweise, dass die juristische Person ungeachtet ihrer räumlichen Aufgliederung als Einheit gelte. Sobald aber die unselbständige Zweigstelle im Ausland angesiedelt ist, gilt sie nach § 2 Abs. 3 Ziff. 2 BDSG als Dritter, d.h. der zwischen der Hauptniederlassung im Inland und der unselbständigen Zweigstelle im Ausland erfolgende Datenaustausch ist als Uebermittlung zu qualifizieren. WITTEK ⁷¹ bestreitet diese Auslegung und stellt diese Uebermittlung von Daten als internen Datenaustausch dar, - auch wenn es sich de facto um einen grenzüberschreitenden Datenverkehr handelt - da die im Ausland gelegene unselbständige Stelle ebenfalls noch Teil der speichernden Stelle sei und deswegen zwischen beiden keine Uebermittlung stattfinde. Er begründet dies damit, dass die Gerichte ⁷² keinen Zweifel daran lassen, dass unselbständige Zweigstellen im Ausland als Teil des in Deutschland ansässigen Hauptunternehmens anzusehen sind. Diese auch für andere rechtliche Vorschriften gültige Regelung ist allerdings nach überwiegender Auffassung der Doktrin aber nicht auf das BDSG anwendbar, da dieser Analogieschluss der ratio legis des BDSG widersprechen würde.⁷³ Eine analoge Anwendung der für die übrigen Rechtsnormen geltenden Regelung würde bedeuten, dass personenbezogene Daten den Geltungsbereich des BDSG ohne jede weitere Prüfung verlassen könnten, wenn sie an eine

68 Vgl. SCHOMERUS, DS+DS 1/80, S. 7f. und WITTEK, DS+DS 2/80, S. 69ff.

69 Vgl. vorne, S. 144.

70 SCHOMERUS, a.a.O.

71 WITTEK, a.a.O., S. 70.

72 Detailangaben, a.a.O.

73 SCHOMERUS, a.a.O.

unselbständige Zweigstelle gesandt werden. Dass die Daten, die in einem Datenverarbeitungssystem jener Zweigstelle im Ausland gespeichert und verarbeitet werden, rechtlich nicht mehr dem Schutz des BDSG unterliegen, ergibt sich aus dem Territorialitätsprinzip. Eine solche Auslegung ist nicht mit dem Schutzzweck des BDSG vereinbar. Auch wenn die Zentrale mit organisatorischen Massnahmen dafür sorgt, dass die in die ausländische Zweigniederlassung übermittelten Daten so geschützt werden, dass ein Missbrauch ausgeschlossen und eine datenschutzkonforme Verarbeitung gewährleistet ist,⁷⁴ kann trotzdem nicht übersehen werden, dass die Daten nicht mehr dem Geltungsbereich des BDSG, sondern den Gesetzen des entsprechenden Landes unterstehen und somit je nachdem geschützt werden - falls ein Datenschutzgesetz existiert - oder schutzlos bleiben. Die organisatorischen Massnahmen stellen eben "nur" Datensicherungsmassnahmen dar, die ohnehin bei der Datenausfuhr zur Vermeidung von Rechtsgutverletzungen aufgestellt werden sollten. Mit Datensicherung alleine vermag man jedoch weder den Geltungsbereich des BDSG auszudehnen, noch die Schutzlosigkeit infolge fehlender rechtlicher Schutznormen im Ausland aufzuheben. Einen Mangel an Schutz gesteht WITTEK⁷⁵ selbst zu, indem er die fehlende Kontrollmöglich- und -tätigkeit der Aufsichtsbehörden im Ausland als Schwachstelle seiner Auffassung bezeichnet: Eine wichtige Institution der Verwirklichung des Datenschutzes sind die Kontrollorgane - wird ihre Tätigkeit durch eine entsprechende Auslegung verunmöglicht, wird der gesetzgeberische Wille missachtet. Der Auffassung WITTEK's, die im Ausland befindliche unselbständige Zweigstelle nicht als Dritter i.S. des § 2 Abs.3 Ziff.2 BDSG zu betrachten, kann nicht zugestimmt werden, da sie die Möglichkeit bietet, Prüfungspflichten, Schutzvorschriften und institutionelle Kontrollen des BDSG zu unterlaufen. Vielmehr ist der Auffassung SCHOMERUS,⁷⁶ beizupflichten und die unselbständige Zweigstelle im Ausland als Dritter zu betrachten, so dass zwischen Zentrale und Zweigstelle eine

74 So der Vorschlag WITTEK's, a.a.O., S. 70.

75 WITTEK, a.a.O.

76 SCHOMERUS, a.a.O., S. 7.

Uebermittlung stattfindet. Aus der Qualifikation des Datentransfers als Uebermittlung folgt, dass die übermittelnde Stelle vor der Weitergabe der Daten prüfen muss, ob die Daten bei der Zweigstelle nach den Vorschriften des BDSG angemessen geschützt sind.⁷⁷ Nur wenn dies bejaht werden kann, dürfen die Daten übermittelt werden. Diese präventive Kontrolle bezweckt das BDSG bei der Uebermittlung von Daten generell, bei der Ausfuhr der Angaben ins Ausland aber im besonderen.⁷⁸

b) Dateneinfuhr

Nebst den Bestimmungen zur Datenausfuhr sind die Bestimmungen über den Schutz-, Anwendungs- und Geltungsbereich des BDSG ebenfalls massgebend, wenn es um die Beurteilung des Schutzzumfanges von importierten personenbezogenen Daten geht. Als positiv ist die Gleichbehandlung von ausländischen und inländischen Daten zu bewerten, weil für den Schutz durch das BDSG letzten Endes entscheidend ist, dass die Verarbeitung der Daten in der BRD stattfindet, ebenso steht die Ausübung der im BDSG verankerten Rechte⁷⁹ In- und Ausländern gleicherweise zu, da es laut Gesetz unerheblich ist, wo das ein Recht wahrnehmende Datensubjekt seinen Wohnsitz hat oder welche Staatsangehörigkeit es besitzt.

Das Gesetz schweigt sich aber darüber aus, inwieweit eine Benachrichtigungspflicht⁸⁰ bei erstmaliger Speicherung von personenbezogenen Daten über ausländische natürliche Personen, die ihren Wohnsitz oder Aufenthalt nicht im Bundesgebiet haben, erforderlich ist. Für die im Inland wohnhaften Ausländer gilt § 26 Abs.1 BDSG (Benachrichtigungspflicht) gleich, wie für die deutschen Staatsangehörigen,

77 Id., S. 8.

78 Die datenschutzrechtliche Prävention stellt eine der wesentlichen Neuerungen gegenüber dem herkömmlichen Recht dar; diese spezielle Präventionsmöglichkeit würde durch die allgemeine Begründung, dass das im Inland befindliche Hauptunternehmen (im Falle einer Persönlichkeitsverletzung durch die Zweigstelle im Ausland) als passivlegitimiert sei, paralysiert.

79 Z.B. ein Recht auf Auskunfterteilung (§ 26 Abs.2 BDSG) und die weiteren Rechte auf Berichtigung, Sperrung, Löschung nach § 27 BDSG.

80 Vgl. §§ 26 Abs. 1 und 34 Abs. 1.

da der Zweck dieser Benachrichtigung darin besteht, den Betroffenen über den Speicherungsort zu informieren, damit er bei Unregelmäßigkeiten die weiteren ihm nach BDSG zustehenden Rechte geltend machen kann. Die Frage nach einer Pflicht zur Benachrichtigung von "ausländischen Staatsangehörigen, die keine persönliche oder sachliche Beziehung zu den Vorgängen in der Bundesrepublik" haben, ist nach SCHWAPPACH⁸¹ zu verneinen, weil der nicht in der BRD wohnhafte ausländische Staatsangehörige wegen fehlender Beziehung kaum von dem mit der Benachrichtigungspflicht verfolgten Zweck Gebrauch machen wird, so dass eine Benachrichtigung nur einen erheblichen, sinnentleerten Aufwand darstellen würde. Die Beurteilung der Benachrichtigungspflicht nach dem Grundsatz der Verhältnismässigkeit zwischen Zweck und Mittel ist ein vertretbares Argument für die Verneinung dieser Frage. M.E. wäre die Lösung, die Benachrichtigungspflicht von einem Anknüpfungspunkt i.S. eines Aufenthaltes oder an ein Vorhandensein von Vermögenswerten innerhalb des Geltungsbereiches des BDSG abhängig zu machen auch tauglich, im Rahmen einer internationalen Konvention verwendet zu werden, um zu einer Klärung dieser Frage beizutragen.

Auch im Bereich der Dateneinfuhr zeigt SCHWAPPACH eine Schwachstelle des BDSG auf: "Verarbeitet die im Inland befindliche Stelle Daten inländischer oder ausländischer Personen im Auftrag eines ausländischen Unternehmens, so stellt der Datenaustausch zwischen diesen Stellen ebenfalls keine Uebermittlung i.S. von § 2 Abs. 2 Ziff. 2 BDSG dar (vgl. § 2 Abs. 3 Ziff. 2 BDSG)."⁸² In diesem Fall kann der Betroffene keine Rechte gegen die im Ausland lokalisierte Gesellschaft anstrengen. Die Argumentation SCHWAPPACHs, dass ein Schutz durch ein deutsches Gesetz nicht notwendig erscheine, weil es sich bei solchen Vorgängen faktisch kaum um die Verarbeitung von Daten inländischer

81 SCHWAPPACH, DS+DS 1/78, S. 23.

82 SCHWAPPACH, a.a.O.

Personen handelt, ist rechtspolitisch nicht haltbar, wenn man einen wirksamen Datenschutz auf nationaler wie internationaler Ebene befürwortet.

Zusammenfassend kann festgestellt werden, dass das BDSG beim grenzüberschreitenden Datentverkehr zwar einen Schutz vorsieht, zu dessen Verwirklichung aber keine ausreichenden Massnahmen zur Verfügung stellt. Weil die Zulässigkeit des Exportes sich allein nach den Voraussetzungen der Zulässigkeit für die Uebermittlung beurteilt,⁸³ existiert kein formalisiertes Verfahren i.S. einer Genehmigung oder Registrierung, das den grenzüberschreitenden Verkehr personenbezogener Informationen einer möglichen Kontrolle unterstellt.⁸⁴ Diese mangelnde Kontrollierbarkeit wird durch die Tatsache, dass im privaten Sektor für die Zulässigkeit der Datenverarbeitung überhaupt kein behördliches Genehmigungs- oder Anmeldeverfahren notwendig ist,⁸⁵ zusätzlich negativ beeinflusst. Anlässlich einer Novellierung des BDSG⁸⁶ wäre es begrüssenswert, wenn eine explizite Regelung des grenzüberschreitenden Datentransfers im Gesetz Eingang finden und die noch vorhandenen Gesetzeslücken in bezug auf den internationalen Datenverkehr (auch hinsichtlich einer Konvention)⁸⁷ durch eine effektivere⁸⁸ Datenschutzkontrolle schliessen würde.⁸⁹

83 Die Tatsache, dass im Destinationsland ein dem BDSG vergleichbares Gesetz in Kraft steht oder nicht, ist dabei zu berücksichtigen.

84 Eine fehlende Kontrollierbarkeit des Datenflusses kann sich vor allem innerhalb der Mitgliedsstaaten einer Konvention negativ auswirken, namentlich wenn sie untereinander den freien Austausch pflegen, gegenüber Nichtmitgliedsstaaten hingegen eine Genehmigung befürworten, damit nicht unkontrolliert Daten aus dem Schutzverbund in "data havens" abfliessen (vgl. STADLER, DS+DS 3/79, S. 169ff.).

85 Vgl. 2. Tätigkeitsbericht d.B.f.D., S. 63ff.

86 Vgl. Synopse der den nichtöffentlichen Bereich betreffenden Novellierungsvorschläge zum BDSG von CDU/CSU vom 24.1.1980 und SPD/FDP vom 27.2.1980 bei DREWS, DS+DS 2/80, S. 89f.; MEISTER, DS+DS 3/80, S. 123ff.

87 Vgl. STADLER, DS+DS 3/79, S. 172f.

88 'Effektiv' ist nicht i.S. von 'restriktiv' zu verstehen.

89 G.L.M.: H.P. Bull, Bundesbeauftragter für Datenschutz: "...the German law needs to be revised to incorporate specific regulation of transborder data flows." in: TDR, Vol. 2, No. 3, S. 1.

2. Oesterreich: Datenschutzgesetz ⁹⁰

A. Allgemeine Grundzüge des DSG

a) Anwendungsbereich

Das DSG schützt grundsätzlich alle personenbezogenen Daten privater und öffentlicher Stellen, die mit Hilfe automationsunterstützter Technologien und Mittel verarbeitet werden.

Die bestehende föderalistische Struktur der Gesetzgebungskompetenz von Ländern und Gemeinden zum Erlass von Datenschutzbestimmungen für die innerhalb ihrer Rechtsträger automationsunterstützt verarbeiteten Daten wurde durch eine kompetenzrechtliche Ergänzung zur Verfassung dem Bund übertragen. Nach § 2 Abs.1 DSG steht dem Bund die ausschliessliche Kompetenz zum Erlass einheitlicher Datenschutzbestimmungen (soweit personenbezogene Daten automationsunterstützt verarbeitet werden) für den gesamten öffentlichen Bereich, d.h. auf Bundes-, Landes- und Gemeindeebene sowie für den privaten Sektor zu.

Mit der Schaffung dieser Verfassungsbestimmung wurde zugleich ein Grundrecht auf Datenschutz verfassungsrechtlich verankert, das jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gibt, soweit er daran ein schutzwürdiges Interesse, insbesondere auf Achtung seines Privat- und Familienlebens, hat.⁹¹

Dieses neu geschaffene Grundrecht hat nun verschiedene Auswirkungen:

- Das Grundrecht verleiht dem verfassungsmässigen Recht auf Datenschutz nicht nur Wirkung gegenüber den öffentlichen Behörden bzw. der Privatwirtschaftsverwaltung,⁹² sondern auch gegenüber Privaten. Diese Drittwirkung gibt einer Person, die behauptet, das Recht auf Geheimhaltung ihrer Daten sei von einem Träger des öffentlichen

90 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG) vom 18. Oktober 1978 (BGBl. 565/1978).

91 § 1 Abs.1 DSG.

92 Verstaatlichte Unternehmen der Privatwirtschaft.

- oder privaten Bereichs⁹³ verletzt worden, die Möglichkeit, auf dem ordentlichen Rechtswege ein Klagebegehren zu stellen.⁹⁴
- Die automationsunterstützte Verarbeitung personenbezogener Daten gibt einen grundrechtlichen Anspruch auf Auskunft, "wer woher welche Daten ermittelt oder verarbeitet, welchen Inhaltes die Daten sind und wozu sie verwendet werden"⁹⁵; zudem besteht auch ein Anspruch auf Richtigstellung unrichtiger oder Löschung unzulässig ermittelter oder verarbeiteter Angaben.
 - Nach STADLER soll dieses Grundrecht "auch im Verkehr zwischen Privaten in den Gerichten zugewiesenen Verfahren Anwendung finden."⁹⁶
 - Das DSG bezweckt mit diesem Grundrecht hauptsächlich die Anwendung auf die automationsunterstützte Datenverarbeitung. Das Grundrecht auf Datenschutz hingegen ist grundsätzlich für alle Arten der Verarbeitung personenbezogener Angaben aufgestellt.⁹⁷ Daraus folgt, dass gegenüber der früheren Rechtslage die Weitergabe personenbezogener Daten, bei denen ein Geheimhaltungsinteresse vermutet wird oder zu vermuten ist, nicht mehr frei erfolgen kann, sondern geprüft werden muss, ob ein Rechtsgrund für deren Weitergabe vorliegt.
 - Als Grundrecht muss es für den Schutz der Daten unerheblich sein, ob die Verarbeitung personenbezogener Informationen im öffentlichen Bereich von Stellen der Bundes-, Landes- oder Gemeindeverwaltung bzw. sonstigen, den verschiedenen Stufen angegliederten Institutionen des öffentlichen Rechts oder innerhalb des privaten Sektors erfolgt. Mit der Ausgestaltung des Schutzes der Privatsphäre als Verfassungsrecht wurde denn auch die rechtliche Voraussetzung für die Schaffung einer einheitlichen Bundeskompetenz zum Schutz der automationsunterstützt verarbeiteten, personenbezogenen Daten ge-

93 Vgl. hinten, S. 161ff.

94 Die gerichtliche Zuständigkeit beurteilt sich nach §29 DSG.

95 PAWLIKOWSKY, DS+DS 1/79, S. 22.

96 STADLER, OeVD 11/78, S. 8.

97 Id., a.a.O.; REISINGER, DS+DS 2/79, S. 122.

bildet. Der Gesetzgeber erachtete es als angebracht, für den Schutz der Privatsphäre ein einheitliches Schutzniveau überall zu verwirklichen und dabei einen gleichartigen Vollzug in allen Bereichen (Bund, Länder, Gemeinden, andere Selbstverwaltungskörper sowie Private) anzustreben.

- Als Voraussetzung für eine Beschränkung dieses Grundrechtes müssen nach § 1 Abs.2 DSG die besonderen, in Art. 8 Abs.2 EMRK genannten Gründe vorliegen.⁹⁸
- Bisher war in Oesterreich nur der öffentlichrechtliche Persönlichkeitsschutz⁹⁹ durch Art. 8 EMRK verfassungsrechtlich abgesichert; die Schaffung des Grundrechts auf Datenschutz, das sowohl zwischen Individuum und Staat als auch zwischen Privaten wirkt, hat nun einerseits im öffentlichrechtlichen Verhältnis eine grundrechtliche Erweiterung der in Art. 8 EMRK enthaltenen Grundsätze gebracht und andererseits zu einer verfassungsrechtlichen Verankerung des zivilrechtlichen Persönlichkeitsschutzes im Hinblick auf den Schutz der Privatsphäre geführt.¹⁰⁰

Analog zu den in der Europäischen Menschenrechtskonvention niedergelegten Grundsätze, kann das Grundrecht auf Datenschutz sowohl von österreichischen Staatsbürgern als auch von Ausländern oder Staatenlosen¹⁰¹ geltend gemacht werden. Voraussetzung ist nur, dass der geltend gemachte Sachverhalt eine Inlandsbeziehung aufweist, die sich aus der territorialen Beschränkung des Geltungsbereiches ergibt.

98 Z.B. Gefährdung der nationalen Sicherheit, öffentlichen Ordnung oder des wirtschaftlichen Wohls, Verhinderung strafbarer Handlungen, Schutz der Rechte und Freiheiten anderer, usw.

99 Art. 8 EMRK bezieht sich nur auf das Verhältnis zwischen Staat und Bürger: "Nur dann, wenn der Staat sich unmittelbar Informationen vom Betroffenen unter Einsatz hoheitlicher Mittel beschafft, kann eine Berührung mit Art. 8 EMRK gegeben sein." (STADLER, Oesterreichisches Datenschutzrecht, S. 50).

100 Vgl. DUSCHANEK, S. 14.

101 Ebenso inländische und ausländische juristische Personen.

Im Gegensatz zu der in Deutschland (im öffentlichen Bereich) herrschenden Subsidiarität des BDSG gegenüber anwendbaren LDSG ergibt sich in Oesterreich aufgrund der anderen kompetenzrechtlichen Regelung ein einheitliches Datenschutzrecht im öffentlichen Bereich; daraus resultiert, dass alle automationsunterstützt verarbeiteten personenbezogenen Daten "den gleichen Schutzvorschriften unterliegen, unabhängig von welcher Behörde und unabhängig für welchen Zweck sie verarbeitet werden."^{102 103} Diese Uniformität der Bestimmungen im öffentlichen Sektor dient der Einfachheit und Uebersichtlichkeit sowohl nach innen wie nach aussen (z.B. in Fragen des grenzüberschreitenden Datenverkehrs), was letztlich der Rechtssicherheit aller mit dem DSG konfrontierten Beteiligten zum Vorteil gereicht.¹⁰⁴

In den Anwendungsbereich des öffentlichen Sektors¹⁰⁵ fallen die personenbezogene Daten verarbeitenden Rechtsträger, die durch Gesetz¹⁰⁶ eingerichtet sind oder von Gesetzes wegen Zwangsbestand haben und hoheitliche Funktionen durchzuführen und zu vollziehen haben.

Die Rechtsträger der öffentlichen Verwaltung,¹⁰⁷ die im privaten Bereich eine "wirtschaftliche Tätigkeit im Rahmen der sogenannten Privatwirtschaftsverwaltung oder in den verschiedenen staatlichen Unternehmen"¹⁰⁸ betreiben, werden nach dem Gleichheitsgrundsatz

102 STADLER, österreichisches Datenschutzrecht, S. 56.

103 Es wurde für die Effektivität des Datenschutzes als entscheidend erachtet, dass gleichartige personenbezogene Angaben gleichrangige Sicherung und Schutz erfahren, so dass auf allen Ebenen der gleiche Rechtsschutz anwendbar ist.

104 Vgl. erwähnte Nachteile bei der föderalistischen Lösung im BDSG; vorne, S. 139f.

105 2. Abschnitt: §§ 6-16 DSG.

106 Bundesgesetz, Landesgesetz.

107 Z.B. unselbständige Anstalten des Bundes, selbständige Anstalten mit eigener Rechtspersönlichkeit, Staatsmonopole, verstaatlichte Wirtschafts- und Kapitalgesellschaften, Gebietskörperschaften, Selbstverwaltungskörper, gesetzliche berufliche Interessenvertretungen sowie andere Rechtsträger des Gesellschaftsrechts.

108 DUSCHANEK, S. 24; STADLER, DS+DS 2/80, S. 91.

sinngemäss den Vorschriften des privaten Bereichs ¹⁰⁹ unterstellt. ¹¹⁰ Die Unterordnung der öffentlichrechtlichen Stellen unter die privatrechtlichen Normen ¹¹¹ des Gesetzes erfolgt über eine funktionelle Abgrenzung mittels der Formel "... soweit sie in Formen des Privatrechts tätig sind ..." ¹¹²; für die ihnen übertragenen hoheitlichen Aufgabenbereiche haben sie sich nach den Bestimmungen des öffentlichen Bereichs zu richten und (damit) den Grundsatz der Gesetzmässigkeit ¹¹³ einzuhalten. ¹¹⁴ Besonderen Bestimmungen unterliegen die für die öffentliche Sicherheit zuständigen öffentlichen Stellen wie z.B. Sicherheitspolizei und Landesverteidigung. ¹¹⁵

Zum privaten Bereich des DSG werden primär alle nicht durch Gesetz geschaffenen Rechtsträger ¹¹⁶ gezählt, d.h. alle dem Privatrecht unterliegenden Rechtsträger wie natürliche oder juristische

109 §§ 4 und 5 DSG schreiben der Bundes- oder den Landesregierungen vor, diese Rechtsträger durch eine konstitutiv wirkende Verordnung von der Anwendung des 2. Abschnittes auszugliedern und dem 3. Abschnitt zu unterstellen.

110 Vgl. Durchführungsverordnungen zum österreichischen DSG.

111 3. Abschnitt: §§ 17-31 DSG.

112 STADLER, OeZW 1979/1, S. 11; ders., DS+DS 2/80, S. 91f.; DUSCHANEK, a.a.O.

113 Vgl. §§ 6 und 7 DSG.

114 Konsequenz dieser Zuweisung zum privaten Bereich ist, dass der im öffentlichen Bereich notwendige Erlass einer Datenschutzverordnung und die Umschreibung der Datensicherungsmassnahmen in einer Betriebsordnung, als Voraussetzung für die Rechtmässigkeit der Datenverarbeitung für den privaten Bereich, entfallen, eine gesetzliche Bestimmung als Grundlage für die Zulässigkeit der Datenverarbeitung ist nicht mehr notwendig. Als Beschwerdeinstanz sind im privaten Bereich anstelle der Datenschutzkommission die ordentlichen Gerichte zuständig. Die Weitergabe von Daten aus dem öffentlichen Bereich eines Rechtsträgers in den zum privaten Teil des DSG zuzurechnenden Bereich sind als Uebermittlungen an Private zu qualifizieren (vgl. STADLER, DS+DS 2/80, S. 91).

115 STADLER, österreichisches Datenschutzrecht, S. 60f.

116 STADLER, OeZW 1979/1, S. 10.

Personen sowie handelsrechtliche Personengesellschaften,¹¹⁷ die personenbezogene Daten innerhalb des räumlichen Anwendungsbereiches des Gesetzes ermitteln, verarbeiten oder übermitteln und die Zulässigkeitsvoraussetzungen der §§ 17, 18 DSG erfüllen. Zusätzlich werden die durch Gesetz eingerichteten Rechtsträger, die in Formen des Privatrechts tätig sind, nach § 4 und 5 DSG dem privaten Sektor unterstellt.

b) Schutzbereich

Das DSG definiert in § 3 Ziff.1 als geschützte personenbezogene Daten,¹¹⁸ die auf einem Datenträger gespeicherten Angaben mit Informationen über bestimmte oder bestimmbare natürliche oder juristische Personen oder handelsrechtliche Personengesellschaften. Damit erstreckt sich der gesetzliche Schutz auch auf personenbezogene Daten juristischer Personen des privaten und öffentlichen Rechts; die handelsrechtlichen Personengesellschaften sind in diesen Schutz ebenfalls eingeschlossen, da sie innerhalb der "österreichischen Rechtsordnung zum Grossteil der juristischen Person des Privatrechts gleichgestellt sind."¹¹⁹ § 3 Ziff.2 nennt als Betroffene denn auch die natürlichen und juristischen Personen und statuiert für sie die Aktivlegitimation zur Geltendmachung der im DSG begründeten Rechte (z.B. Auskunftsrecht §§ 11, 25 DSG).

Im Gegensatz zum BDSG wird im österreichischen DSG der Kollektivdatenschutz verwirklicht; der Gesetzgeber rechtfertigt diesen Schutz mit der Begründung, dass die Mehrheit von Informationen über eine juristische Person Rückschlüsse auf natürliche Personen zulässt "und

117 Vereine, politische Parteien, gemeinnützige Genossenschaften, gesetzlich anerkannte Kirchen, Privatpersonen, am wirtschaftlichen Wettbewerb beteiligte Gesellschaften und Unternehmen, etc.

118 Zum Begriff personenbezogene Daten vgl. REISINGER, Begriffsfeld Datenschutz, S. 31.

119 DUSCHANEK, S. 19.

die Datenverarbeitung andererseits eine Bedrohung auch von Kollektivinteressen darstellt."¹²⁰ Diese umfassende Regelung beseitigt die beim BDSG genannten Nachteile¹²¹ zugunsten einer grösseren Rechtssicherheit und breiteren Schutzwirkung.¹²²

c) Geltungsbereich

Das in § 1 Abs.1 statuierte Grundrecht auf Datenschutz gilt für alle Arten der Verarbeitung personenbezogener Daten, somit für manuelle und automationsunterstützte Verfahren.

Das DSG selbst beschränkt seinen Geltungsbereich auf den automationsunterstützten Datenverkehr,¹²³ der in den verschiedenen Phasen der Ermittlung,¹²⁴ Verarbeitung,¹²⁵ Uebermittlung¹²⁶ und Löschung¹²⁷ teils manuell, teils automatisiert durchgeführt werden kann.¹²⁸ Diese oft untrennbare Mischung von automationsunterstütz-

120 Id., a.a.O.

121 Vgl. vorne, S. 140f.

122 Das von Gegnern des Kollektivdatenschutzes vorgebrachte Argument, dass gerade die juristischen Personen und Personengesellschaften die Privatsphäre bedrohen, ist m.E. kein Grund, ihnen den Schutz personenbezogener Daten vorzuenthalten.

123 Unter dem Terminus 'Datenverkehr' definiert das Gesetz in § 3 Ziff.10 die Ermittlung, Verarbeitung, Benützung, Uebermittlung von personenbezogenen Daten oder Behandlung mit nur einer dieser Funktionen. Der Begriff 'Datenverkehr' ist dem der 'Datenverarbeitung' im BDSG gleichzustellen.

124 Ermitteln i.S. von § 3 Ziff.5 DSG beinhaltet sowohl das automationsunterstützte Erfassen, als auch das nicht automatisierte Erheben und sonstige Beschaffen von personenbezogenen Angaben (z.B. durch Ausfüllen von Fragebogen, etc.).

125 Unter Verarbeiten i.S. von § 3 Ziff.6 DSG sind die automationsunterstützten Teil-Funktionen des Speicherns, Ordners, Veränderns, Vervielfältigens, Ausgebens und Löschsens zusammengefasst. Dabei gibt es jedoch Ueberschneidungen bei der online-Datenverarbeitung, wo die Datenerhebung, Datenerfassung, Dateneingabe, Verarbeitung, Löschung und Verknüpfung in einem Arbeitsprozess, d.h. ohne logische Trennung der verschiedenen Phasen erfolgt.

126 Uebermitteln i.S. von § 3 Ziff.8 umfasst die automationsunterstützten oder manuellen Teil-Funktionen des Weitergebens, Uebertragens, Veröffentlichens, Bekanntgebens oder anderer Offenbarungsarten für Dritte, d.h. andere Destinatäre als Auftraggeber,

ten und nicht automatisierten Teilfunktionen und Vorgängen führte zu dem Bestreben, jede Form der automationsunterstützten Datenverarbeitung in den Geltungsbereich miteinzubeziehen, um Umgehungsmöglichkeiten auszuschliessen: es resultierte die Lösung, dass das Datenschutzgesetz auf alle Phasen des Datenverkehrs (auch die manuellen) Anwendung findet, falls ein Datum auch nur in einer einzigen Phase automationsunterstützt, d.h. mit vorgegebenem Programm und maschinell, verarbeitet wird.¹²⁹ Entscheidend für die Anwendung des Gesetzes wird somit nicht primär ein einzelner konkret zu beurteilender, automationsunterstützter Vorgang oder Teilfunktion, sondern die Tatsache, dass die Daten in irgendeiner Phase einer programmgesteuerten, maschinellen Verarbeitung unterzogen werden.¹³⁰ Damit wurde der Geltungsbereich des DSG sehr weit gefasst¹³¹ und Umgehungsmöglichkeiten erschwert; die Regelung hat den Vorteil der Einfachheit und kann auf zusätzliche, komplizierende Begriffe wie denjenigen der 'Datei' im BDSG verzichten.

Verarbeiter oder Betroffener. Eine Kreuzung mit der Verarbeitungsphase besteht bei der Verknüpfung von ermittelten Daten eines Aufgabenbereiches mit denen eines anderen Bereiches. Die Verknüpfung selbst wird unter den Vorgang des Uebermittels subsumiert.

127 Unter Löschen i.S. von § 3 Ziff.9 wird das Unkenntlichmachen von erfassten oder gespeicherten Daten für den nichtautomationsunterstützten wie automatisierten Datenverkehr verstanden. Das in Ziff.6 aufgeführte Löschen ist als Teilfunktion des Verarbeitungsvorganges zu verstehen und erfolgt dort immer automationsunterstützt.

128 Vgl. REISINGER, Begriffsfeld Datenschutz, S. 35ff.

129 DUSCHANEK, S. 22; STADLER, österreichisches Datenschutzrecht, S. 57; PAWLIKOWSKY, DS+DS 1/79, S. 22.

130 STADLER, Versicherungsrundschau, S. 244.

131 Nicht erfasst werden damit praktisch nur die herkömmlichen Notizbücher und einfachen Handkarteien, die auf keine Art automationsunterstützt bearbeitet werden können. Wenn aber von einer automationsunterstützten Seite her (z.B. Computerausdruck) der Hinweis oder Verweis auf die Benützung einer Handkartei erfolgt, fällt auch die Handkartei als verwiesener Bereich unter den Geltungsbereich des DSG (vgl. STADLER, a.a.O.). Vom Gesetz betroffen wird zweifelsfrei die computerisierte Informationsverarbeitung, mittlere Datentechnik und bis zu einer gewissen Untergrenze auch die automationsunterstützte Textverarbeitung.

B. Rechtliche Regelung des grenzüberschreitenden Datenverkehrs

Als hervorstechender Unterschied des DSG gegenüber dem BDSG ist das Vorhandensein eines speziellen Abschnittes mit spezifischen Bestimmungen zum internationalen Datenverkehr zu nennen. Die im 4. Abschnitt aufgeführten Normen ermöglichen folgende Einteilung:

- Export von Daten: §§ 32, 34 Abs. 1 DSG,
- Import von Daten: §§ 33, 34 Abs. 2 DSG.

a) Datenexport

§ 32 DSG regelt die Voraussetzungen für die Ueberlassung von Daten ins Ausland.

aa) Allgemeines

Der Begriff "Ueberlassung" dient als Sammelbegriff für alle Formen des grenzüberschreitenden Datentransfers ins Ausland, so dass alle möglichen Phasen der Verarbeitung auf irgendeinem Teil der Transportstrecke - ohne Beschränkung auf spezifische Funktionen, die nur grenzüberschreitend durchführbar sind - erfasst werden. Somit fällt auch die Benutzung ausländischer Datenverarbeitungsdienste durch inländische Unternehmen unter den Tatbestand der Ueberlassung. Voraussetzung ist, dass eine Auslandsbeziehung herrscht, die aber schon dann gegeben ist, wenn mit Ausnahme eines einzigen Vorganges alle übrigen im Inland erfolgen: daraus resultiert, dass § 32 DSG anwendbar ist, sobald mindestens eine Phase der Datenverarbeitung im Ausland vorgenommen wird, wie auch dann, wenn eine Ueberlassung¹³² zum Zwecke der Durchführung aller Verarbeitungsschritte im Ausland erfolgt.

Der Wortlaut des Abs. 1 hingegen beschränkt die Ueberlassung auf automationsunterstützt verarbeitete Daten und erfasst nicht die mit manuellen (nicht automationsunterstützten) Funktionen bearbeiteten Daten, die zur Weiterverarbeitung ins Ausland übermittelt werden.

¹³² Die Datenerfassung wird von einem österreichischen Rechtsträger durchgeführt, aber alle folgenden Verarbeitungsvorgänge werden im Ausland vollzogen.

Eine Ausklammerung der im Inland manuell verarbeiteten Daten - mit nachfolgenden automationsunterstützten Phasen im Ausland - vom Geltungsbereich des Gesetzes eröffnet Umgehungsmöglichkeiten dergestalt, dass die in Oesterreich manuell durchgeführten Funktionen als vorbereitende Handlungen für nachfolgende automationsunterstützte Verarbeitungsschritte im Ausland dienen könnten. Die ratio legis zielt aber nicht auf eine so restriktive Auslegung dieses Absatzes, sondern erheischt eine analoge Beurteilung des Geltungsbereiches des Gesetzes für nachfolgende Auslandsbearbeitungen in dem Sinne, dass die Anwendbarkeit des DSG auch dann gegeben sein soll, wenn die innerhalb Oesterreich erfolgten Bearbeitungsphasen manueller Natur sind, aber einer der nachfolgenden oder bereits vorgenommenen Schritte im Ausland automationsunterstützt abläuft.¹³³ Dies wird durch die Bestimmung von § 32 Abs. 3 Ziff. 4 DSG erhärtet, bei dem die im Ausland erfolgende Verarbeitung als Dienstleistung i.S. der §§ 13 und 19 DSG keinen Unterschied für die Anwendbarkeit von § 32 DSG für die mit automationsunterstützten bzw. manuellen Verfahren bearbeiteten Daten setzt.¹³⁴ STADLER¹³⁵ stellt fest, dass unter § 32 DSG nicht nur die Uebermittlung in den verschiedenen Formen der Datenverarbeitung fällt, sondern auch die Ueberlassung von maschinell erstellten Ausdrucken oder die Ueberlassung von Daten auf noch nicht maschinell lesbaren Datenträgern zum Zwecke ihrer Verarbeitung im Ausland. Somit wird nach dem für das DSG skizzierten Geltungsbereich¹³⁶ auch die nicht automationsunterstützt erfolgte Uebermittlung nach dem DSG be-

133 Vgl. STADLER, OeZW 1979/1, S. 14: "Die Uebermittlung von automationsunterstützt verarbeiteten Daten ist auch dann nach dem DSG zu beurteilen, wenn sie selbst nicht automationsunterstützt erfolgt, aber die Daten aus einer solchen Verarbeitung stammen."

134 Vgl. DUSCHANEK, S. 60: er qualifiziert die Formulierung als 'missglückt'.

135 STADLER, österreichisches Datenschutzrecht, S. 67; gl. M. BEDNAR/WEISSENBOECK, S. 206.

136 Vgl. vorne, S. 164f.

urteilt, sofern die Daten aus einer Verarbeitung mit automationsunterstützten Vorgängen stammen oder solche nachfolgen.

§ 32 DSG ist für die in den §§ 4, 5 und 17 DSG genannten Rechtsträger, d.h. für den Export personenbezogener Daten von öffentlichen und privaten Stellen anwendbar. Die geltenden Zulässigkeitsvoraussetzungen für die Ueberlassung von Angaben sind analog den für das Inland geltenden Uebermittlungsbestimmungen der §§ 7 und 18 DSG zu beurteilen; dadurch wird die Ueberlassung folgerichtig an die Voraussetzungen der Uebermittlung geknüpft. Die analoge Anwendung der für die Uebermittlung im Inland geltenden Voraussetzungen auf diejenigen des Datenexportes vermeidet eine unnötige Komplizierung der Vorschriften und fördert die Einfachheit der Anwendung.

Der Aufzählung einzelner Voraussetzungen zur Uebermittlung sei aber zunächst eine nähere Erläuterung des Begriffes 'Uebermittlung' vorausgeschickt. Dabei fällt auf, dass die Terminologie des DSG nicht vergleichbar ist mit derjenigen des BDSG¹³⁷ und daraus eine rechtlich unterschiedliche Behandlung in gleichen Situationen resultieren kann.¹³⁸

bb) Bestimmung des Begriffes 'Uebermitteln'

Als Uebermittlung i.S. des DSG wird grundsätzlich die Weitergabe personenbezogener Daten in irgendeiner Form von einem (vom Auftraggeber verschiedenen)¹³⁹ Rechtsträger an einen andern Rechtsträger verstanden. Somit ist der Datenaustausch zwischen einem Konzern angehörigen Gesellschaften oder den in einem organschaftlichen Verhältnis befindlichen Unternehmungen als Uebermittlung zu qualifizieren, da

137 Vgl. vorne, S. 143f.

138 Eine störende Tatsache, die (bei einer internationalen Konvention oder) in einem internationalen Rechtsregime durch Vereinheitlichung der Begriffsstruktur oder zumindest mittels materiellrechtlich ausgleichenden Regelungen zu vermeiden versucht werden sollte.

139 Ausnahmefall: vgl. nachfolgend, S. 170.

diese rechtlich unabhängig sind und eigene Rechtspersönlichkeit besitzen, demzufolge als selbständige Rechtsträger gelten. (Ein Kriterium für das Vorliegen einer Uebermittlung ist somit die Eigenschaft, nach österreichischem Recht als Rechtsträger eingestuft zu werden).¹⁴⁰

Innerhalb des Rechtsträgers dürfen die personenbezogenen Daten durch dessen Angestellte benutzt oder an Zweigstellen¹⁴¹ übertragen werden, soweit sie in demjenigen Aufgabenbereich verwendet werden, für den sie zulässigerweise ermittelt oder verarbeitet wurden. Werden hingegen die Daten von einer Abteilung an eine oder mehrere Abteilungen mit einem andern, unterschiedlichen Aufgabenbereich innerhalb des gleichen Rechtsträgers übergeben, liegt ebenfalls eine Uebermittlung i.S. des Gesetzes vor. "Die Behandlung eines solchen 'Verknüpfens' als Uebermitteln, obwohl ein Rechtsträger nicht verlassen wird, hat den Zweck, den Zusammenhang der Daten mit dem Ermittlungsgrund zu wahren."^{142 143 144} Der Begriff 'Uebermitteln' umfasst somit nicht nur die allgemeine Erscheinung des Weitergebens von Daten an einen andern Rechtsträger, sondern auch den speziellen Fall der Verwendung der für einen bestimmten Aufgabenbereich ermittelten bzw. verarbeiteten Daten für Zwecke eines andern Aufgabengebietes.

Eine Ausnahme vom Grundsatz der Uebermittlung als Weitergabe von Daten an einen andern Rechtsträger bildet die als Dienstleistung erfolgte Verarbeitung von Daten: die vom Auftraggeber dem verarbeitenden

140 Für Beschreibung von Beispielen vgl. STADLER, Versicherungsrundschau, S. 248.

141 Die Zweigstellen gelten in Oesterreich nicht als juristisch selbständige und unterschiedliche Rechtsträger.

142 STADLER, österreichisches Datenschutzgesetz, S. 14.

143 Demnach wäre der Austausch der Kundendateien innerhalb der Abteilungen eines Unternehmens mit organisatorisch eigenständigen, getrennten Bereichen zum Verkauf von Schreibmaschinen und Computern ein 'Uebermitteln' i.S. des Gesetzes.

144 Uebermittlungsbegriff in der öffentlichen Verwaltung: "Uebermittlung an Dritte ist gleichzuhalten, die Verwendung von für ein Aufgabengebiet ermittelten Daten in einem anderen Aufgabengebiet derselben Behörde." (STADLER, Verwaltungspraxis, S. 12).

den Rechtsträger zur Erfüllung der Dienstleistung übertragenen Daten bzw. die Rückgabe der Informationen, welche einer oder mehreren Verarbeitungsphasen unterzogen worden sind, an den Auftraggeber, wird nicht als Uebermittlung i.S. von §§ 7 und 18 DSG qualifiziert. Erfolgt nach der Verarbeitung der Daten durch den Verarbeiter eine Weitergabe der Daten an einen vom Auftraggeber bestimmten Dritten, so liegt im Verhältnis Auftraggeber und Verarbeiter keine Uebermittlung, sondern eine 'Ueberlassung' vor; hingegen ist im Verhältnis Verarbeiter bzw. Auftraggeber und dem Dritten eine Uebermittlung anzunehmen. Voraussetzung der 'Ueberlassung' ist lediglich, dass ein 'Rechenzentrumsvertrag'¹⁴⁵ zur Verarbeitung und zur Behandlung der Daten zwischen Auftraggeber und Verarbeiter i.S. von § 19 DSG abgeschlossen wurde. Der Vertrag muss die (notwendige) Verpflichtung des Verarbeiters beinhalten, die Daten ausschliesslich nach den Weisungen des Auftraggebers zu behandeln, bzw. zu verwenden und allgemeine oder besondere Verschwiegenheitspflichten sowie Datensicherungsmassnahmen einzuhalten. Beim Verarbeiter sollte ausserdem eine Qualifikation in der Weise vorliegen, dass er im Datenverarbeitungsregister eingetragen ist.¹⁴⁶ Treten bei der Verarbeitung Unregelmässigkeiten auf und ergeben sich daraus Schäden für die Betroffenen, so ist ein trotz Nichteintragung des Verarbeiters im Datenverarbeitungsregister erteilter Verarbeitungsauftrag als Verletzung der Sorgfaltpflicht auf Seiten des Auftraggebers zu werten.

Im Zusammenhang mit der Datenverarbeitung als Dienstleistung ist die oben erwähnte Ausnahme vom Begriff der 'Uebermittlung' analog auf die Fälle anzuwenden, bei denen innerhalb eines Konzerns Daten verschiedener Gesellschaften einem speziell geführten Konzernrechenzentrum zur zentralisierten Verarbeitung weitergegeben werden und

145 STADLER, OeZW 1979/1, S. 17.

146 Vgl. auch § 23 DSG.

dieses die verarbeiteten Daten wieder ausschliesslich an die die entsprechenden Informationen führenden Gesellschaften (Auftraggeber) zurücksendet. Zur rechtlichen Absicherung empfiehlt STADLER die Aufnahme des Geschäftszweckes¹⁴⁷ in die Statuten oder Satzung der verarbeitenden Stelle: "Um die Zulässigkeit solcher Datenübermittlungen ausser Zweifel zu stellen, sollten diese in der Rechtsgrundlage für die jeweils bestehende Unternehmensverflechtung (z.B. Beherrschungsvertrag) ausdrücklich verankert werden (mit Hinweisen wie z.B. 'zwecks Führung einer gemeinsamen Verkaufsorganisation' oder 'zwecks Führung einer gemeinsamen Personalverwaltung')."¹⁴⁸ Auch in diesem Falle kann nicht von einer Uebermittlung i.S. des Gesetzes gesprochen werden und die Verarbeitung der Daten von mehreren Unternehmen in einem gemeinsamen Rechenzentrum ist ebenfalls nach § 19 DSG als Dienstleistung im Datenverkehr zu beurteilen.

cc) Materielle Zulässigkeitsvoraussetzung der Uebermittlung im öffentlichen Bereich

§ 7 DSG setzt alternativ sechs verschiedene Kriterien, die in einer internen Datenschutzverordnung (§ 9) umschrieben sein müssen, für die Zulässigkeit der Uebermittlung von personenbezogenen Daten eines öffentlichen Rechtsträgers an eine andere öffentliche Stelle voraus:¹⁴⁹

1. Gemäss Legalitätsprinzip ist einer öffentlichen Stelle die Uebermittlung von Daten, die sich auf eine ausdrückliche gesetzliche Ermächtigung abstützt, immer erlaubt.
2. Der zweite Uebermittlungsgrund ist die schriftliche Zustimmung des Betroffenen, dem aber jederzeit ein Widerspruchsrecht (ebenefalls auf schriftlichem Wege) offensteht.

147 In diesem Fall wäre der Geschäftszweck des verarbeitenden Unternehmens die Dienstleistung der zentralisierten Verarbeitung von Daten für andere Konzerngesellschaften.

148 STADLER, a.a.O., S. 16.

149 Id., österreichisches Datenschutzrecht, S. 58f.

3. Zulässig ist die Uebermittlung, wenn personenbezogenen Daten durch Anonymisierung jede Bestimmbarkeit zu einer Person genommen wurde, so dass per definitionem keine personenbezogenen Daten mehr übermittelt werden.
4. Als Ausnahme bereichsspezifischen Charakters ist die Uebermittlung von Daten einer öffentlichen Stelle an eine Kreditunternehmung des öffentlichen oder privaten Rechts zulässig, falls diese mit der Auszahlung von Geldleistungen im Zusammenhang stehen.¹⁵⁰ Eine Gefährdung dieser personenbezogenen Daten ist deshalb als gering zu qualifizieren, weil die Kreditinstitute zur Wahrung des Bankgeheimnisses verpflichtet sind.
5. Ein weiterer Uebermittlungsgrund bildet der Transfer personenbezogener Daten an das Oesterreichische Statistische Zentralamt, das die Daten in der Folge anonymisiert verarbeitet.
6. Abs. 2 gibt einen weitgefassten Grund der Zulässigkeit der Uebermittlung von Daten, wenn sie für den Empfänger als Organ einer Bundes-, Landes- oder Gemeindestelle bzw. Körperschaft des öffentlichen Rechts zur Erfüllung seiner gesetzlich übertragenen Aufgabe eine wesentliche Voraussetzung darstellen. Eine solche Voraussetzung wird immer dann gegeben sein, wenn die Daten mit den zu erfüllenden Behördenaufgaben direkt im Zusammenhang stehen und die Durchführung der Behördentätigkeit auf einer gesetzlichen Grundlage beruht (Legalitätsprinzip).

Die Uebermittlung von personenbezogenen Daten durch öffentliche Rechtsträger an private Stellen wird nur aus den ersten vier skizzierten Gründen erfolgen und ist bei Vorliegen der Voraussetzungen auch zulässig.

150 Diese Vorschrift bezieht sich auf die Uebermittlung von Gehaltsangaben von im öffentlichen Bereich angestellten Arbeitnehmern an Kreditinstitute.

dd) Materielle Voraussetzungen der Uebermittlung im privaten Bereich

Als Vorbedingung jeder Uebermittlung nennt § 18 DSG die grundsätzliche Zulässigkeit der Verarbeitung von Daten beim übermittelnden Rechtsträger; als Korrelat zur Uebermittlung muss aber auf der Seite des Empfängers ebenfalls sowohl die Ermittlung wie die Verarbeitung von Daten zulässig sein.

Grundvoraussetzung für eine zuverlässige Uebermittlung personenbezogener Daten im privaten Bereich bilden einerseits gesetzliche Uebermittlungspflichten¹⁵¹ (§ 18 Abs.2) oder andererseits die (eben erwähnte) Zulässigkeit der Verarbeitung personenbezogener Daten (nach § 17) sowie das Fehlen gesetzlicher Verschwiegenheitspflichten.¹⁵² Kumulativ zu diesen letzteren Vorbedingungen sind noch weitere Voraussetzungen zu erfüllen, die in vier Gruppen unterteilt werden können:¹⁵³

- Schutzwürdige Belange des Betroffenen müssen beachtet werden und dessen ausdrückliche, schriftliche Zustimmung¹⁵⁴ zur Uebermittlung vorliegen.
- Die zweite Gruppe für die Zulässigkeit von Uebermittlungen wird nach dem Rahmen des berechtigten Zweckes des Rechtsträgers beurteilt, d.h. die Uebermittlung muss zum Geschäftszweck des Rechtsträgers gehören. Dadurch werden all diejenigen Uebermittlungen zulässig, die zur Erfüllung von Verträgen mit dem Datensubjekt als notwendig erscheinen. Umgekehrt werden alle Uebermittlungen personenbezogener Informationen, die nicht auf einem Vertragsverhältnis oder auf dem als 'Uebermittlung personenbezogener Daten' bezeichneten Geschäftszweck basieren, grundsätzlich unzulässig.

151 Z.B. Meldepflichten an gesetzliche Sozialversicherungsträger.

152 Dies bedeutet, dass gesetzliche Verschwiegenheitspflichten (Ärzte, Rechtsanwälte, etc.) den Bestimmungen über die Zulässigkeit von Uebermittlungen nach § 18 DSG vorgehen.

153 STADLER, österreichisches Datenschutzgesetz, S. 16ff.

154 Die Zustimmung ist jederzeit schriftlich widerruflich, auch befristete oder bedingte Zustimmungserklärungen sind denkbar.

- Die Uebermittlung wird auch immer dann zulässig sein, wenn sie zur Wahrung überwiegender Interessen eines Dritten notwendig ist. Diese Beurteilung bedingt aber vorerst eine Interessenabwägung zwischen Betroffenen und Dritten, wobei die des letzteren überwiegen müssen. Als überwiegend können nur diejenigen Interessen bezeichnet werden, die von der Rechtsordnung anerkannt sind, d.h. die im Zusammenhang mit dem rechtlichen Zweck einer Unternehmung bereits bei der Zulässigkeit der Datenverarbeitung positiv beurteilt wurden. Als Indizien für das Vorhandensein eines überwiegenden Interesses können z.B. offene Forderungen aus einem Vertrag angesehen werden oder Angaben, die in Verbindung mit einer Zession stehen, etc. Im Zweifelsfall muss die Entscheidung gemäss dem Grundsatz von § 1 Abs. 2 DSG im Interesse des Persönlichkeitsschutzes zugunsten des Betroffenen gefällt werden.
- Ebenfalls zulässig ist die Uebermittlung, falls Daten in anonymisierter Form transferiert werden, so dass der Betroffene nicht mehr bestimmbar ist, d.h. die übermittelten Angaben dürfen keine individualisierenden Merkmale mehr aufweisen.

ee) Formale Voraussetzungen für die Zulässigkeit von Uebermittlungen ins Ausland

aaa) Grundsatz

Für die Uebermittlung bzw. Ueberlassung von personenbezogenen Daten ins Ausland muss gemäss § 32 Abs. 1 DSG von den Verarbeitern des öffentlichen wie des privaten Bereiches grundsätzlich eine Bewilligung der Datenschutzkommission¹⁵⁵ eingeholt werden. "Genehmigungspflichtig wird nicht der einzelne Ueberlassungsakt sein, sondern es wird von einem Antrag auf Genehmigung der Ueberlassungen von deren erstmaliger Durchführung auszugehen sein."¹⁵⁶ Die Genehmigung bezieht sich somit auf bestimmte Datenarten bzw. Datenkategorien,

155 Ausführungen zum Tätigkeits- und Aufgabenbereich der Datenschutzkommission, vgl. REISINGER, DS+DS 2/79, S. 123.

156 STADLER, österreichisches Datenschutzrecht, S. 67.

Datenträger und gewisse Arten von Empfängern,¹⁵⁷ so dass eine erteilte Genehmigung zu einer mehrmaligen Ueberlassung von personenbezogenen Daten unter den gleichen Bedingungen berechtigt. Es wird auch der Begriff 'Mustergenehmigung',¹⁵⁸ verwendet, was darauf hinweist, dass die einem Unternehmen eines gewissen Wirtschaftsbereiches für bestimmte Datenarten erteilten Genehmigungen als Vorlage für die übrigen antragstellenden Gesellschaften dieses Wirtschaftsbereiches dienen können.

Auf die Erteilung der Genehmigung besteht ein Rechtsanspruch,¹⁵⁹ wenn folgende Bedingungen gemäss § 32 Abs. 3 DSG seitens des Auftraggebers bzw. des Ueberlassenden kumulativ erfüllt sind:

- Die Zulässigkeitsvoraussetzungen der Uebermittlung i.S. von § 7 bzw. 18 müssen vom öffentlichen und privaten Rechtsträger erfüllt sein.¹⁶⁰
- Es dürfen keine völkerrechtlichen Verpflichtungen¹⁶¹ oder öffentlichen Interessen¹⁶² einer Genehmigung entgegenstehen.

157 Die Datenverarbeitungsregister-Verordnung (BGBI. Nr. 573/1979) enthält einen besonderen Teil für die Registrierung im Zusammenhang mit dem internationalen Datenverkehr. Bei der Einholung der Genehmigung ist zu spezifizieren, an welchen Ort (Staat) Daten exportiert werden, welche Personenkreise von der Uebermittlung betroffen sind, welche und wieviele Verarbeitungsvorgänge im Ausland oder für das Ausland stattfinden etc.

158 STADLER, Versicherungsgrundschau, S. 255.

159 § 32 Abs. 3 i.V. mit Abs. 1 DSG.

160 Vgl. vorne, cc) und dd), S. 171f. und 173f.

161 Als völkerrechtliche Verpflichtung wäre z.B. eine internationale Datenschutz-Konvention denkbar, innerhalb der - zwecks Verhinderung von "data havens" - der Export von Daten eines Mitgliedstaates durch einen andern als den Ursprungsstaat (der Datenbank bzw. Daten) an einen Nichtkonventionsstaat grundsätzlich untersagt ist, um die Authentizität der Daten zu garantieren. Dem Ursprungsland, d.h. demjenigen Staat, in dem die Datenbank lokalisiert ist, könnte unter den Konventionsmitgliedern freilich nicht das Recht abgesprochen werden, seine Daten auch einem Nichtmitgliedstaat zu übermitteln, ohne ihn eines souveränen Entscheidungsrechtes zu berauben.

- Der Auftraggeber bzw. Uebermittelnde muss glaubhaft machen, dass keine schutzwürdigen Interessen des Betroffenen durch die Datenausfuhr tangiert werden. Hier ist eine gewisse Redundanz feststellbar, da die Beachtung der schutzwürdigen Belange bereits als Zulässigkeitsvoraussetzung für die Verarbeitung und Uebermittlung aufgestellt wurde.
- Bei der Ueberlassung von Daten zwecks Benutzung einer Dienstleistung im Ausland i.S. von § 19 muss sichergestellt sein, "dass der ausländische Verarbeiter dieselben Pflichten akzeptiert, wie der inländische."¹⁶³ Für den die Daten exportierenden Auftraggeber in Oesterreich bedingt diese Vorschrift den Abschluss eines Rechenzentrumsvertrages mit einem ausländischen Verarbeiter in gleicher Weise wie bei einer Auftragserteilung an ein inländisches Service-rechenzentrum.¹⁶⁴ Es ist ratsam, die in § 19 DSG enthaltenen Pflichten (Rückgabe der Daten bzw. der Ergebnisse der Verarbeitung, Verschwiegenheits- und Sorgfaltspflichten etc.) im Rechenzentrumsvertrag zu integrieren, um die in § 34 Abs.3 Ziff.4 aufgestellte Bedingung für eine Genehmigung zur Ueberlassung ins Ausland zu erfüllen.

Falls eine der vorhergenannten Bedingungen nach § 32 Abs. 3 DSG fehlt, liegt es im Ermessen der Datenschutzkommission, eine Genehmigung zu erteilen. Die Entscheidung der Kommission über einen Antrag auf Genehmigung¹⁶⁵ muss innerhalb von sechs Monaten erfolgen.¹⁶⁶

bbb) Ausnahme

In Abs. 2 des § 32 DSG sind die Ausnahmefälle aufgeführt, bei denen die grundsätzliche Genehmigung für den Datenexport nicht erforderlich ist:

162 Z.B. die nationale Sicherheit bei Daten der Landesverteidigung.
163 SUERBOECK, S. 56.

164 Vgl. vorne, S. 170.

165 Dem Antrag sollten die nach § 32 Abs. 3 DSG notwendigen Angaben beigelegt werden, damit die Datenschutzkommission eine Prüfung der Kriterien für die Genehmigung vornehmen kann.

166 STADLER, österreichisches Datenschutzrecht, S. 67.

- Der Hauptfall ist in Ziff. 2 zu finden: ein (genehmigungs-)freier Export personenbezogener Daten ist mit Empfängern innerhalb derjenigen Staaten möglich, in denen für personenbezogene Daten ein durch das österreichische Gesetz verwirklichter Datenschutz in vergleichbarer Form Anwendung findet.

BEDNAR/WEISSENBOECK halten es jedoch für ratsam, die Kommission auch beim Export in Staaten mit vergleichbaren Datenschutzregelungen solange einzuholen, "bis durch eine Verordnung die Gleichwertigkeit ausländischer Datenschutzbestimmungen (gemäß § 32 Abs. 5) festgestellt wird."¹⁶⁷ Diese Verordnung wird vom Bundeskanzler nach Anhörung der Datenschutzkommission erlassen. Damit wird auch ein Entscheid darüber zu fällen sein, welche Modalitäten erforderlich sind, um Informationen über juristische Personen an Empfänger in Deutschland, Frankreich oder Schweden ¹⁶⁸ zu übermitteln, da in diesen Ländern die personenbezogenen Daten über juristische Personen nicht unter den Schutzbereich der geltenden Datenschutzgesetze fallen. Nach STADLER ¹⁶⁹ ist für diese Staaten beim Export personenbezogener Angaben zu juristischen Personen eine Genehmigung der Datenschutzbehörde nach den allgemeinen, grundsätzlichen Kriterien erforderlich, da ein genehmigungsfreier Export solcher Daten in diese, zu den sechs wichtigsten Handelspartnern Österreichs zählenden Länder eine Umgehung des österreichischen Gesetzes fördern würde.¹⁷⁰ Eine solche Umgehungsmöglichkeit wäre deshalb von praktischer Bedeutung, weil bei Handelsbeziehungen vor allem die Angaben zu juristischen Personen und handelsrechtlichen Personengesellschaften von besonderem Interesse sind.

167 BEDNAR/WEISSENBOECK, S. 207.

168 Ders. (S. 203) führt als die sechs wichtigsten Handelspartner Österreichs folgende Rangliste auf:
1. BRD; 2. Italien; 3. Schweiz; 4. Grossbritannien; 5. Frankreich; 6. Schweden.

169 STADLER, Wirtschaftsbrief 1979/11-12.

170 Vgl. den Begriff "small data havens", vorne, S. 44f.

Dies bedeutet nach dem gegenwärtigen Stand der Rechtslage, dass personenbezogene Angaben über natürliche Personen ohne Genehmigung seitens der österreichischen Datenschutzkommission nach Deutschland,¹⁷¹ Schweden und Frankreich übermitteln können; nach Norwegen und Luxemburg ist der Datentransfer von Informationen über natürliche wie auch über juristische Personen frei.

- Betreffen die aus Oesterreich auszuführenden Daten den Auftraggeber selbst, ist laut § 32 Abs.2 Ziff.1 keine Genehmigung erforderlich. Dieser Fall wird häufig bei internationalen Gesellschaften auftreten, wenn österreichische Tochtergesellschaften oder Niederlassungen ihre eigenen Unternehmensdaten (z.B. Verkaufs-, Produktions- und Finanzdaten) zur Konsolidierung an den Hauptsitz oder eine andere nationalen Gesellschaft¹⁷² ins Ausland übermitteln. Dabei ist aber darauf zu achten, dass die exportierten Datenbestände nicht auch Informationen über einzelne Kunden, Lieferanten oder andere Personen enthalten: die Anwendbarkeit von Ziff. 1 ist nur dann gegeben, wenn die Angaben ein bestimmtes Datensubjekt betreffen und dieses zugleich identisch mit dem Auftraggeber der Uebermittlung ist. Diese restriktive Auslegung bezweckt einerseits einen erleichterten Datenexport multinationaler Firmen an andere zum Konzern gehörenden Gesellschaften im Ausland, andererseits wird verhindert, dass zusammen mit diesen den Ausführenden selbst betreffenden Daten noch Informationen zu andern Rechtssubjekten ohne Genehmigungspflicht ausgeführt werden.
- Als dritter Ausnahmefall wird nach § 32 Abs.2 Ziff.3 auf die Einholung einer Genehmigung verzichtet, falls dies in völkerrechtlichen Vereinbarungen vorgesehen wird. Diese Norm verrät gesetzgeberische Weitsicht, vor allem im Hinblick auf eine internationale Konvention, deren allgemein anerkannte Zielsetzung ein von Bewilligungs-

171 Detaillierte Ausführungen bei STADLER, a.a.O.

172 Meistens wird diese Gesellschaft auch zum Konzern gehören, muss es aber nicht.

pflichten und Genehmigungsschranken freier Datenexport innerhalb der Mitgliedstaaten sein müsste. Diese Regelung schafft damit eine Voraussetzung für den Anschluss der österreichischen Datenschutzgesetzgebung an eine künftige internationale Konvention mit dem darin verwirklichten Postulat des freien Datenaustausches unter den Konventionsstaaten.

ccc) Weitere formelle Vorschriften

Hat die Datenschutzkommission die Genehmigung zum Export von Daten erteilt, falls eine solche notwendig war, müssen die Datenverarbeiter bzw. Auftraggeber gemäss § 32 Abs. 4 die vorgesehene Uebermittlung bzw. Ueberlassung der personenbezogenen Daten im Datenverarbeitungsregister protokollieren¹⁷³ lassen. Diese Vorschrift betrifft alle öffentlichen datenverarbeitenden Stellen; im privaten Bereich sind hingegen nur diejenigen Rechtsträger betroffen, für die nach §§ 22 Abs. 4 und 23 DSG eine Registrierungspflicht¹⁷⁴ besteht. Nach Erhalt der Registermitteilung samt Registerauszug dürfen die Daten ins Ausland transferiert werden.¹⁷⁵ Laut Gesetz (§ 47 Abs. 4) darf die Uebermittlung bzw. Ueberlassung nicht ohne Registernummer des inländischen Datenverarbeiters erfolgen. Es existiert aber keine dem § 22 Abs. 1 entsprechende Informationspflicht der Betroffenen bei einem Export von Daten.

ff) § 34 Abs. 1 DSG

Ebenfalls unter den Export von Daten wird die Regelung des § 34 Abs. 1 DSG subsumiert. Einerseits wiederholt er die aus dem Geltungs-

173 Die Protokollierung einer konkreten Uebermittlung kann nach STADLER (OeZW 1979/1, S. 17, Anm. 32) auch durch eine generell-abstrakte Angabe von Empfängern ersetzt werden.

174 Formale Voraussetzung für die Zulässigkeit der Datenverarbeitung (für fremde Zwecke und in bestimmten Fällen auch für eigene Zwecke) ist die Registrierung beim Datenverarbeitungsregister nach §§ 8, 22 Abs. 4, 23 i.V. mit 47 DSG; aufgrund dieses Registerseintrages wird eine Registernummer (§ 47 Abs. 4) erteilt, die zur Aufnahme der Echtverarbeitung berechtigt.

175 BEDNAR/WEISSENBOECK, S. 208.

bereich resultierende Folgerung,¹⁷⁶ dass die Datenexportbestimmungen auch dann Anwendung finden, wenn einzelne Arbeitsvorgänge ins Ausland verlagert werden. Andererseits setzt er fest, dass der Direktzugriff von im Ausland befindlichen Datenstationen auf Datenbanken in Oesterreich den gleichen Voraussetzungen und Bestimmungen unterliegen soll wie der Export von Daten gemäss § 32 DSG. Letztere Regelung ist sicherlich sinnvoll, da es sich beim Direktzugriff auf im österreichischen Bundesgebiet gelegenen Datenbanken technisch ebenfalls um einen Datenexport handelt, wobei die exportierende Stelle aber nicht in Oesterreich lokalisiert ist, sondern vom Ausland aus tätig wird. Würde der vom Ausland her zugreifende Verarbeiter weniger streng oder anders behandelt, würde dadurch eine Umgehungsmöglichkeit der Art eröffnet, dass statt der Ausfuhren durch im Inland befindliche Rechtsträger Datenbanken aufgebaut würden, die vom Ausland aus abgefragt werden könnten; ausserdem würde eine mögliche Rechtsunsicherheit gefördert. Den vom Ausland auf in Oesterreich befindliche Datenbanken erfolgende Direktzugriff als Ueberlassung zu qualifizieren, ist die konsequente, logisch richtige Lösung.

b) Datenimport

§ 33 DSG regelt den Datenimport bzw. die Verarbeitung personenbezogener Daten innerhalb von Oesterreich für ausländische Rechtsträger.

aa) Allgemeines

Die Bestimmung betrifft den Fall, bei dem ein im österreichischen Hoheitsgebiet befindlicher Rechtsträger personenbezogene Daten für ein ausländisches Rechtssubjekt importiert und sie im Inland verarbeitet. Der Verarbeiter in Oesterreich wird für einen ausländischen Rechtsträger tätig, von dem aber im Gesetz nicht gesagt ist, wo er sich befindet. Logischerweise, d.h. aufgrund der Lokalisation der Be-

176 Vgl. vorne, S. 168.

stimmung im 4. Abschnitt,¹⁷⁷ ist anzunehmen, dass mit dem Begriff 'ausländischer Rechtsträger' ein im Ausland befindlicher (nicht österreichischer) Rechtsträger verstanden wird.

bb) Materielle Voraussetzung

Aus der Gesetzesformulierung geht deutlich hervor, dass für die Anwendbarkeit von § 33 DSG ein Dienstleistungsvertrag (z.B. ein Rechenzentrumsvertrag) eines ausländischen Rechtsträgers mit einem in Oesterreich lokalisierten Rechenzentrum bzw. Dienstleistungsunternehmen vorliegen muss. Nach Regelung des Gesetzes hat dabei der ausländische Auftraggeber auf die Einhaltung der Zulässigkeitsvoraussetzungen für die Verarbeitung von Daten i.S. von §§ 17 i.V. mit 19 DSG zu achten.¹⁷⁸ Für den Auftraggeber im Ausland wird es allerdings schwierig sein, die Zulässigkeitsvoraussetzungen für die Verarbeitung von Daten und die damit zusammenhängenden Normen des DSG vollumfänglich zu erfassen. Diese Regelung kann grundsätzlich den Datenimport nach Oesterreich zwecks Verarbeitung in einem Rechenzentrum behindern, weil die Einhaltung der gesetzlichen Voraussetzungen einerseits profunde Kenntnisse des österreichischen Datenschutzgesetzes und andererseits ein nach dem DSG konformes Verhalten im Ausland voraussetzt. Diese fachliche Ausdehnung des Anwendungsbereiches des DSG über das nationale Hoheitsgebiet hinaus kann u.U. zu Konflikten auf Seiten des Auftraggebers führen, wenn das ihm vom DSG auferlegte Verhalten und Handeln im Widerspruch zu Bestimmungen seines nationalen Datenschutzgesetzes oder anderer Erlasse am Orte seines Geschäftssitzes steht.

cc) Formelle Voraussetzungen

Bedingung für die Verarbeitung der Daten, welche von einem im Ausland befindlichen Rechtsträger stammen, ist eine Meldung des österreichischen Dienstleistungsverarbeiters an das Datenverarbeitungsre-

177 Falls ein ausländischer Rechtsträger seinen Sitz in Oesterreich hat, sind die Normen des internationalen Datenverkehrs nicht anwendbar, da es sich in diesem Fall um nationalen Datentransfer handelt.

178 SUERBOECK, S. 56.

gister: "Zu beachten ist, dass auch der Verarbeiter mit Gewerbeberechtigung, der sonst nicht registrieren müsste, zur Meldung verpflichtet ist."^{179 180}

Die Meldepflicht besteht aber nur bei der Einfuhr von Daten zwecks Verarbeitung als Dienstleistung in Oesterreich. Gemäss § 47 Abs. 5 ist dem Anmelder die Durchführung des Eintrages mittels eines Registerauszuges mitzuteilen, was ihn zur Aufnahme der tatsächlichen Verarbeitung für den ausländischen Rechtsträger berechtigt.

Diese Meldepflicht ist vor dem Hintergrund verständlich, dass bei der Datenverarbeitung als Dienstleistung nach § 19 DSG die Daten wieder an den Auftraggeber zurückerstattet werden müssen. Die Rückerstattung selbst ist zwischen Verarbeiter und Auftraggeber nicht als Uebermitteln i.S. des Gesetzes,¹⁸¹ sondern als Ueberlassung zu qualifizieren, für deren Zulässigkeit wiederum die Voraussetzungen von § 32 gegeben sein müssen. Der Eintrag im Datenverarbeitungsregister bringt damit einen gewissen Ausgleich gegenüber der im Inland geltenden Regel, den Eintrag als Qualifikation für die Uebernahme von Verarbeitungsaufträgen zu werten.¹⁸² Analog zur nationalen Ebene, wird auch ein entsprechender Eintrag im Datenverarbeitungsregister und dessen Beachtung bzw. Nichtbeachtung durch ausländische Auftraggeber als Erfüllung bzw. Missachtung der Sorgfaltspflicht bei der Bewertung von Unregelmässigkeiten zu beurteilen sein. Darin ist als Reflexwirkung letztlich auch ein Schutz der Daten zugunsten ausländischer Rechtsträger enthalten.

In Satz 2 wird als Voraussetzung zum Datenimport eine Genehmigung der Datenschutzkommission vorgeschrieben, wenn eine solche in völkerrechtlichen Verträgen vorgesehen ist. Zur Zeit gibt es allerdings keine derartigen völkerrechtlichen Vereinbarungen.

179 SURBOECK, S. 56; ebenso DUSCHANEK, S. 62.

180 Vgl. auch § 23 Abs. 3 DSG.

181 Vgl. vorne, S. 190ff.

182 Vgl. vorne, S. 169f.

dd) § 34 Abs. 2 DSG

Ebenfalls unter den Begriff des Datenimportes fällt die Bestimmung von § 34 Abs. 2, die den Direktzugriff von Oesterreich aus auf ausländische Datenbanken ebenfalls dem § 33 unterstellt. Damit werden auch die von Oesterreich aus erfolgenden Zugriffe auf im Ausland gespeicherte personenbezogene Angaben der Meldepflicht an das Datenverarbeitungsregister (bzw. der Genehmigungspflicht durch die Datenschutzkommission gemäss völkerrechtlichen Verträgen) unterstellt. Die formellen Voraussetzungen sind für beide Tatbestände identisch, was nur der Praktikabilität zuträglich sein kann. Materiellrechtlich bringt dieser Absatz aber keine bedeutende Erweiterung im Personenkreis gegenüber § 33. Während in § 33 DSG nach dem genauen Wortlaut des Gesetzes nur die in Oesterreich befindlichen Rechtsträger der Meldepflicht unterstehen, die für ausländische Auftraggeber Daten verarbeiten, erfasst der Kreis der Normadressaten in § 34 Abs.2 nun auch diejenigen, die nicht aufgrund eines Dienstleistungsvertrages auf Daten im Ausland zurückgreifen: damit erstreckt sich dieser Absatz auf die grössere Zahl der Verarbeiter, die zu eigenen (oder fremden) Zwecken einen direkten Zugriff auf im Ausland befindliche, personenbezogene Daten vornehmen.

Der Verweis auf § 33 DSG ist aber nicht in dem Sinne restriktiv interpretierbar, dass mit § 34 Abs. 2 nur diejenigen österreichischen Rechenzentren angesprochen sein sollen, die - basierend auf einem Dienstleistungsvertrag - für einen ausländischen Verarbeiter einen direkten Zugriff auf Daten im Ausland vornehmen. Eine solche Auslegung des Gesetzes würde an den datenverarbeitungsmässigen Realitäten und Gepflogenheiten vorbeigehen. Vielmehr wird hier die in § 33 DSG für den Spezialfall der grenzüberschreitenden Inanspruchnahme einer Dienstleistung in Oesterreich aufgestellte Meldepflicht (bzw. Genehmigungspflicht) auf den Normalfall der Datenverarbeitung zu eigenen Zwecken ausgedehnt und analog angewendet.

c) Exkurs: Begriffsbestimmung des 'direkten Zugriffs'

Unklarheit ¹⁸³ herrscht ebenfalls in der Auslegung des Begriffes 'direkter Zugriff'. Der Ausdruck stammt aus der EDV-Terminologie

und bezieht sich auf eine der Methoden (direkte, sequentielle), der Uebertragung von Daten zwischen Hauptspeicher und den peripheren Einheiten.

Als direkter Zugriff wird der Vorgang der Gewinnung von Daten aus dem Hauptspeicher bzw. die Eingabe von Daten in den Speicher bezeichnet, die auf die Art erfolgt, dass die Zugriffszeit von der Lage des Datums auf dem Speicher(medium) weitgehend unabhängig ist. Verständlicher wird die Umschreibung anhand des Mediums: Speichermedium für einen direkten Zugriff bilden z.B. die Magnetplatten (Disks); die EDV erlaubt hier den Zugriff auf ein Datum direkt, d.h. für alle auf dem Datenträger befindlichen Daten praktisch gleich schnell, somit zeitunabhängig. Das Gegenstück bilden z.B. die Magnetbänder (Tapes), die für die Abfrage von Daten aus dem gespeicherten Datenbestand ein sequentielles Durchlaufen des ganzen Bandes voraussetzen, bis man beim gesuchten Datum angelangt ist. Für die am Anfang des Bandes erscheinenden Daten ist die 'Zugriffszeit' viel kürzer, als für die am Ende des 'Tapes' gespeicherten Angaben. Denkbar ist aber auch, dass ein Band in den Hauptspeicher eines Computers eingelesen wird und innerhalb dieses Computerspeichers ein direkter Zugriff erfolgen kann.¹⁸⁴

M.E. bringt aber eine technisch konzise Auslegung wenig, so dass eine allgemeine, prinzipiengemässe Umschreibung verständlicher und zutreffender ist: als "direkten Zugriff" sind all jene Vorgänge zu qualifizieren, bei denen von einem Computersystem (über eine Verbindung) mittels Datenfernverarbeitung auf den Datenbestand eines Computersystems¹⁸⁵ gegriffen werden kann.¹⁸⁶ Konkret kann dies mit

183 Unklarheit ist anzunehmen, weil nirgends in der mir bekannten österreichischen Literatur zum Datenschutz eine Begriffsbestimmung des 'direkten Zugriffs' zu finden war.

184 In der Regel ist der Datenbestand von international zugänglichen Datenbanken auf 'Disks' oder Massenspeicherm Medien gespeichert, da sie den technisch 'direkten' Zugriff und damit kurze Antwortzeiten ermöglichen.

185 Für die Anwendbarkeit von § 34 muss sich eines der Computersysteme mit der angeschlossenen Datenbank im Ausland befinden.

186 Zum Verständnis der Vorgänge vgl. die Beschreibungen des IBM-Datennetzes; vorne, S. 73ff.

folgendem Beispiel ausgedrückt werden: Greift eine österreichische Muttergesellschaft mit ihrem in Oesterreich stehenden Computersystem über eine Telefonverbindung (Wahl- oder Mietleitung) direkt auf gespeicherte personenbezogene Daten eines von der Tochtergesellschaft in der Schweiz betriebenen und gelegenen Datenverarbeitungssystems, damit sie diese schweizerischen Daten zusammen mit den andern personenbezogenen Informationen auf dem österreichischen Computersystem verarbeiten kann, ist der Tatbestand des § 34 Abs. 2 DSG erfüllt, d.h. die Aufnahme der Verarbeitung der importierten Daten aus der Schweiz kann erst nach Erfüllung der Meldepflicht i.S. von § 33 i.V. mit § 34 Abs. 2 DSG und Erhalt des Registerauszeuges erfolgen.

Anhand dieses Beispiels wird auch ersichtlich, dass es für den direkten Zugriff unerheblich ist, ob die personenbezogenen Daten von einem 'Disk' direkt abgerufen werden können (dies ist bei dialogmässigen Datenbankabfragen die Regel), oder ob durch die gegebenen Möglichkeiten der Fernverarbeitung zuerst bestimmte Vorgänge im Ausland veranlasst werden müssen (z.B. sequentielles Einlesen von Tapes in den Hauptspeicher und eventuelle weitere Arbeitsschritte), damit die benötigten Daten importiert werden können. Eine technisch orientierte Auslegung würde ein zu restriktives Spektrum erbringen und zukünftige technische Erweiterungsmöglichkeiten oder gewisse Verarbeitungsmethoden von der Anwendbarkeit des § 34 ausschliessen.

C. Folgerung

- Die Regelung des grenzüberschreitenden Datenverkehrs im DSG ist positiv zu beurteilen. Die sichtbare Hervorhebung der Regelung im 4. Abschnitt unterstreicht einerseits die Bedeutung des internationalen Datentransfers und beweist andererseits gesetzgeberische Weitsicht, die auch in materiellrechtlicher Hinsicht, mit dem Einbezug einer zukünftigen internationalen Konvention oder völkerrechtlicher Verträge, unter den übrigen Datenschutzgesetzen hervorsticht und - so ist zu hoffen - eine Signalwirkung haben wird.
- Im Zusammenhang mit dem Datenexport und vor allem -import ist grundsätzlich zu bemerken, dass das DSG auf die gesamte innerhalb des österreichischen Hoheitsbereiches erfolgende Verarbeitung

personenbezogener Daten anwendbar ist, so dass es für die Schutzwirkung des Gesetzes keine Rolle spielt, ob die Daten österreichische oder ausländische Staatsangehörige oder nicht in Österreich wohnhafte Personen betreffen.¹⁸⁷ Dadurch wird auch ohne internationale Vereinbarungen sowohl für die Ein- als auch Ausfuhr von personenbezogenen Informationen bereits ein möglicher Ansatzpunkt für Umgehungen ausgeschaltet.

- Die Anwendbarkeit der §§ 32 bis 34 für den öffentlichen wie privaten Bereich trägt entscheidend zu deren einfacheren Beurteilung und Handhabung durch einheimische und ausländische Stellen bei. Die Rechtssicherheit wird zusätzlich verstärkt, indem für den gesamten öffentlichen Bereich einheitliche Normen gelten und die mit einer föderalistisch-strukturierten Lösung verbundenen Nachteile der Vielfalt von Instanzen und Gesetzesvorschriften vermieden werden.
- Die Schaffung eines einzigen Aufsichtsgremiums, der Datenschutzkommission, die für alle Bereiche in Fragen der Genehmigung oder Zulassung auf nationaler wie internationaler Ebene zuständig ist, bringt eine erleichterte Orientierbarkeit für das Ausland und trägt zur Rechtssicherheit im Beurteilungs- und Genehmigungsverfahren bei.
- Durch das Genehmigungssystem kann von der mit Fachexperten besetzten Datenschutzkommission der Datenausfuhr ein Riegel vorgeschoben werden, falls sich erweisen sollte, dass über bestimmte Kanäle das Gesetz umgangen werden könnte. Dieses behördliche Durchgriffsrecht fehlt im BDSG.
- Der gesetzlich verankerte Rechtsanspruch auf eine Genehmigung (falls die Voraussetzungen nach § 32 Abs. 3 DSG erfüllt sind), hat nach SURBOECK¹⁸⁸ zur Folge, dass die Einholung der Genehmigung in den meisten Fällen nur einen Formalakt darstellt. M.E. dient dieser Rechtsanspruch auch dazu, Willkürakte der Datenschutzkommission grundsätzlich zu verhindern, soweit sie angesichts des Grundsatzes der Gleichbehandlung aller Antragstellenden möglich sind;

187 Gleiche Regelung wie im BDSG, vgl. vorne, S. 156.

188 SURBOECK, S. 56.

ausserdem wird damit eine zu restriktive Handhabung des Datenexportes vermieden. Der Vorteil dieses Genehmigungssystems besteht darin, dass ein Abwehrdispositiv gegen einen unkontrollierten Datenausfluss aufgestellt wird, dieses aber nur zur Anwendung kommt, wenn das Persönlichkeitsrecht einer oder mehreren Personen gefährdet ist. Besteht keine Gefährdung, weil im Ausland durch ein vergleichbares Gesetz oder durch einen völkerrechtlichen Vertrag der Schutz der Daten gewährleistet ist, ist der Datenfluss frei.

- Im Zusammenhang mit der Erteilung einer Genehmigung ist die Ausfertigung einer Mustergenehmigung erwähnt worden:¹⁸⁹ "Hier ist an Mustergenehmigungen gedacht, die zweckmässigerweise im Rahmen einer Interessenvertretung verarbeitet werden sollten. Das würde ihnen und uns das Leben erleichtern, dass die Datenschutzkommission dann einige Mustergenehmigungen etwa für Rückversicherungen im Bereich einer bestimmten Art editiert, und dass dann diese Mustergenehmigungen eben für sämtliche Versicherungsunternehmungen angewandt werden."¹⁹⁰ Bei den Mustergenehmigungen gibt es zwei vordergründige Problempunkte, die beachtet werden sollten: für Mustergenehmigungen spricht das Prinzip der Rechtsgleichheit; gegen diese, die Gefahr der Verwässerung der Kontrolle.
- Im Gegensatz zum Export personenbezogener Daten gibt es keine grundsätzliche Genehmigungspflicht für Import von Daten. Sie ist nur in diejenigen Fällen vorgesehen, bei denen völkerrechtliche Verträge zur Anwendung kommen und eine Genehmigung vorsehen.¹⁹¹ Die

189 Vgl. vorne, S. 175, Anm. 158.

190 STADLER, Versicherungsgrundschau, S. 255.

191 Nicht vorstellbar wäre eine solche Genehmigungspflicht m.E. in einer internationalen Konvention unter den Mitgliedstaaten: Man kann im Rahmen einer internationalen Konvention nicht freien Datenexport postulieren und gleichzeitig die Einfuhr personenbezogener Daten von Genehmigungen abhängig machen, da beide Genehmigungspflichten den freien Datenverkehr unter Mitgliedsländern behindern. Allenfalls ist eine solche Importgenehmigung gegenüber Nichtmitgliedstaaten denkbar, m.E. aber ebenfalls nicht sinnvoll, da die Daten vom geschützten oder ungeschützten Ausland mit Eintritt ins österreichische Hoheitsgebiet automatisch dem DSG unterstellt sind und, falls sie unter den Konventionsstaaten ausgetauscht werden, ebenfalls unter Schutz stehen.

Meldepflicht ans Datenverarbeitungsregister beim Import (§ 33) entspricht der Registrierungspflicht beim Export nach § 32 Abs. 4 DSG.

- Als geglückte Regelung ist die Schaffung der Registernummer und die Vorschrift zur Beifügung dieser Nummer bei Uebermittlungen im In- und ins Ausland sowie Mitteilungen an den Betroffenen usw. zu werten. Ein "Indossament" von Registernummern kann helfen, die komplizierten Wege der Verarbeitung, denen Daten unterzogen werden, leichter zu rekonstruieren und eventuelle Schwachstellen ausfindig zu machen bzw. auszuschalten. Die Bedeutung einer solchen Registernummer der Verarbeiter ist vielleicht erst in der praktischen Erfahrung erkennbar, für den Verarbeiter bedeutet sie keine direkte Belastung und ist leicht beizufügen, dem betroffenen Datensubjekt gewährt sie erhöhte Sicherheit beim Umgang mit den Datenverarbeitern und dient ihm als zusätzliche Stütze bei der Wahrnehmung seines Persönlichkeitsrechtes. Es wäre wünschenswert, wenn dieses Beispiel auf internationale Nachahmung stossen würde, so dass die nationalen wie internationalen Verarbeitungen unterzogenen Daten ein lückenloses Indossament ihrer Verarbeiter und Verarbeitungsschritte aufweisen würden. Die Beifügung der Registernummer bei Uebermittlungen ins Ausland ist ein singulärer und positiv zu wertender Vorstoss.

3. Internationale Uebersicht

A. Allgemeines

Eine Analyse der weiteren in Europa existierenden Datenschutzgesetze, entsprechend dem deutschen und österreichischen Gesetz, würde den Rahmen dieser Arbeit sprengen. Ich beschränke meine ausführlichen Betrachtungen deshalb auf die beiden genannten Gesetze und stelle die Regelung des grenzüberschreitenden Datenverkehrs der übrigen Gesetze summarisch dar. Die ebenfalls innerhalb dieses Paragraphen erfolgende Typenbeschreibung¹⁹² der rechtlichen Ausgestaltung des grenzüberschreitenden Datenverkehrs wird zusätzliche Angaben zu den aufgeführten Gesetzen enthalten.

B. Gesetzesmodelle

Beim Vergleich der verschiedenen Datenschutzgesetze ist die unterschiedliche Konzeption im Lösungsansatz des Datenschutzes generell mitzuberücksichtigen, da gerade im Bereich des grenzüberschreitenden Datenverkehrs Unterschiede in der materiellrechtlichen Konkretisierung auftauchen, welche nur durch die Typisierung des Gesetzesmodelles verständlich werden.

a) Institutionelles Modell

Das institutionelle Modell wird charakterisiert durch ein Rahmengesetz, das in seiner materiellrechtlichen Ausgestaltung nur sehr allgemein und teilweise rein programmatisch gehalten ist. Dieser institutionelle Lösungsansatz basiert auf der Ansicht, dass materielle Regelungen zur Gestaltung des Datenschutzes wegen der Relativität der Persönlichkeitssphäre nur sehr allgemein gehalten sein können.¹⁹³

¹⁹² Vgl. nachfolgend III., S. 220ff.

¹⁹³ SCHOMERUS, DS+DS 2/78, S. 62.

Ein Hauptpunkt des Rahmengesetzes besteht in der Schaffung eines institutionellen Organs (Datenschutzkontrollinstanzen),¹⁹⁴ das mit umfassenden Gewalten (Kontrolle, Einsicht, Genehmigung, Instruktion von Beschwerden etc.) und Aufgaben ausgestattet ist. Eine der wichtigsten Aufgaben besteht darin - dort, wo das Gesetz dem Aufsichtsorgan diese Kompetenz überträgt - die allgemeinen gesetzlichen Formulierungen durch materiell- und formellrechtliche Ausführungsbestimmungen zu konkretisieren, da (nach dieser Auffassung) eine Konkretisierung des Gesetzes immer erst im Hinblick auf bestimmte Datentypen und Verarbeitungsmodalitäten erfolgen kann. Zum Aufgabenkreis des Organs kann auch die Durchsetzung von Rechten der Bürger gegenüber datenverarbeitenden Stellen gehören. Der von der Datenverarbeitung in seinen Rechten verletzte Bürger setzt u.U. sein Recht, das er aus dem Gesetz oder den Ausführungsbestimmungen herleitet, nicht direkt gegenüber dem Anwender durch, sondern das Aufsichtsorgan vollzieht die Durchsetzung. Die Befugnisse dieser Kontrollbehörden sind aber unterschiedlicher Natur und von Gesetz zu Gesetz verschieden ausgestaltet.

b) Organisatorisches Modell

Das organisatorische Modell ist gekennzeichnet durch ein Regelwerk, d.h. das Gesetz regelt die Datenschutzmaterie durch grundlegende, detaillierte und ausführliche materiell- und formellrechtliche Vorschriften; dabei bringen bereichs- und fachspezifische Spezialbestimmungen die entscheidenden Einschränkungen gegenüber den grundlegenden systematischen Normen.¹⁹⁵

Auch im organisatorischen Lösungsmodell existiert ein institutionelles Organ, es kommt ihm aber nicht eine solch zentrale Bedeutung zu: Seine Gewalt ist nicht so umfangreich wie im institutionellen Modell, da z.B. der Erlass von Ausführungsbestimmungen weitgehend

194 1. Tätigkeitsbericht d.B.f.D., S. 54.

195 Aus diesem Grund kommen DSG und BDSG einander im Ansatz am nächsten.

durch die grundlegende materielle Ausgestaltung des Regelwerkes vorweggenommen wurde. Der Tätigkeitsbereich des Aufsichtsorgans beinhaltet hauptsächlich Aufsichts-, Kontroll- und Genehmigungsfunktionen, häufig ist das Organ auch Beschwerdeinstanz und zuständig für die Beobachtung der Datenschutzentwicklung. Die betroffenen Bürger leiten i.d.R. ihre Individualrechte direkt aus dem Gesetz und setzen sie selbst gegenüber den Datenverarbeitern durch. Das Aufsichtsorgan ist im organisatorischen Modell mit weniger Aufgaben betraut, hat allerdings bezüglich der Kontrollaufgaben in beiden Modellen beinahe die gleichen Befugnisse.

Von diesen unterschiedlichen Lösungsansätzen einer Datenschutzgesetzgebung existieren die verschiedensten Ausprägungsformen: innerhalb des Spektrums beider Reinformen sind auch Mischformen möglich.

C. Schweden

a) Export personenbezogener Daten

Das schwedische Datenschutzgesetz ¹⁹⁶ bestimmt in § 11, dass personenbezogene Daten nur nach einer Genehmigung durch die Datenschutzbehörde ins Ausland übermittelt werden dürfen.

Der Genehmigungspflicht unterliegen in erster Linie Daten, die auf automationsunterstützten Medien ¹⁹⁷ gespeichert werden und zur Datenverarbeitung ins Ausland übermittelt werden sollen. Die Uebertragung von Informationen über eine in Schweden befindliche Datenstation, die mit einem Computer im Ausland verbunden ist, wird ebenfalls unter diese Bestimmung subsumiert. Der umgekehrte Fall des (Direkt-) Zugriffs von einer Datenstation im Ausland auf ein in Schweden lokalisiertes Datenverarbeitungssystem fällt unter die erste Gruppe. VINGE ¹⁹⁸ führt aus, dass auch der parallele Fall unter die Genehmigungspflicht des § 11 einzureihen ist, bei dem die Uebermittlung der

196 "Lag om endrig i datalagen" (1973:289:SFS 1979:334).

197 Tapes, Disks, Disketten, Massenspeichermedien etc.

198 VINGE, S. 63.

Daten ins Ausland nicht computerisiert erfolgt, sondern von einem in schwedischem Hoheitsgebiet stehenden Computer gedruckt und in Form von Listen bzw. anderen Computerausdrucken zur nachfolgenden Datenverarbeitung ins Ausland exportiert wird. Auch der Austausch personenbezogener Informationen über eine (direkte) Verbindung zwischen zwei Computersystemen ist nach § 11 zu beurteilen.

Hingegen fällt die Uebergabe und Auslieferung von manuell erstellten Quellinformationen und -dokumenten zum Zwecke der Datenverarbeitung im Ausland nicht unter die Genehmigungsvorschrift.^{199 200} Nach Ansicht des schwedischen Gesetzgebers werden die Ergebnisse einer solchen Verarbeitung vom Gesetz nicht betroffen, wenn sie als Ausdruck nach Schweden zurückübertragen werden; anders ist die Sachlage hingegen, wenn sie auf Datenverarbeitungsmedien gespeichert wird.

Dieser partielle Schutz ist m.E. nur fragmentarisch und verursacht eine Datenleckstelle oder sog. "data gaps" durch die personenbezogene Angaben auf manuell erstellten Erhebungslisten ins Ausland gelangen und dort entsprechend verarbeitet werden können. Hier wird wieder offensichtlich, dass nicht nur die automationsunterstützte, sondern auch die manuellen Verarbeitungsarten unter den Schutzbereich des Gesetzes fallen müssen, um mögliche Datenlücken zu vermeiden. Solche entstehen zwangsläufig, wenn nur die automationsunterstützten Verarbeitungsschritte vom Gesetz erfasst werden, während die mit manuellen Methoden erstellten Datenbeständen frei zur elektronischen Verarbeitung im Ausland ausgeführt werden können.

Die schwedische Datenschutzbehörde hat allerdings gemäss § 18 die Möglichkeit, von ihr erlassene Regelungen abzuändern oder neue Bestimmungen herauszugeben, soweit dies zum Schutz gegen Eingriffe in die Privatsphäre von Individuen notwendig ist.²⁰¹

199 Vgl. VINGE, a.a.O.

200 Hier besteht z.B. ein Unterschied zum österreichischen DSG, das auch manuell erfasste Daten schützt, wenn diese zum Zweck der automationsunterstützten Verarbeitung ins Ausland übermittelt werden.

201 Ausfluss des institutionellen Modells.

Die für den Export der Daten notwendige Genehmigung ist grundsätzlich nicht als Mustergenehmigung,²⁰² sondern als Einzelgenehmigung ausgestaltet. Die Datenschutzbehörde prüft jeden Antrag auf Datenausfuhr individuell und bewertet dabei verschiedene wichtige Punkte wie z.B. das Risiko unsachgemässer Handhabung im Destinationsland, ferner das innenpolitische Stimmungsbild und die Beunruhigung angesichts dieser Risiken auf Seiten der Öffentlichkeit, sowie den Umfang der Datensicherungsmaßnahmen und die damit für jeden individuellen Fall verwirklichte Sicherheit der Daten.²⁰³ Eine entscheidende Rolle bei der Beurteilung einer Genehmigungserlaubnis spielt das Grundprinzip, dass der grenzüberschreitende Datenverkehr dann gestattet werden soll, wenn sichergestellt ist oder zumindest eine relative Gewissheit besteht, dass für die Verarbeitung der weitergegebenen Daten Grundsätze und Bestimmungen vorhanden sind, die den für das Inland aufgestellten Schutzprinzipien entsprechen. Dies ist die Richtschnur, die das Gesetz der Datenschutzbehörde bei der Beurteilung von Genehmigungen als allgemeine Orientierungsklausel bietet.

In der bisherigen Praxis war die Haltung der Datenschutzbehörde bei Genehmigungen zur Ausfuhr, wie die Kasuistik²⁰⁴ zeigt, vor

202 Ausnahmefälle sind aber möglich, vgl. z.B. die schwedischen SWIFT-Mitgliederbanken (cf. Anm. 204).

203 VINGE, S. 57.

204 Zur Kasuistik vgl. VINGE, S. 57ff; TDR, Vol.1, No.3, June 78, S. 4/6; Information Privacy, Vol.1, No.1, Sept. 1978, S. 12/13; vgl. auch vorne, S. 12, Anm. 18.

Einige Beispiele verweigerter und genehmigter Exportbewilligungen personenbezogener Daten veranschaulichen die praktischen Überlegungen und die Haltung der Datenschutzbehörde:

- In zwei gleichgelagerten Fällen wurde mit den Entscheidungen vom 12.8.74 und 27.8.74 der Export einer grossen Menge personenbezogener Daten nicht genehmigt, weil einerseits das die Daten importierende Land kein Datenschutzgesetz besass, andererseits bei der grossen Menge der betroffenen Personen (ca. 80'000) leicht Kopien der schwedischen Einwohnerregister hätten hergestellt und mit bestehenden Datenbanken zur Er-

allem zu Beginn ihrer Tätigkeit sehr restriktiv. Diese vorsichtige Haltung wuchs vor allem aus der Besorgnis, grosse Teile der Bevölkerung auf ausländischen Datenbanken abgebildet zu haben und dadurch in ein potentiell²⁰⁵es Abhängigkeitsverhältnis zu geraten, ausserdem könnte sich die Bevölkerung in ihrer Privatsphäre gefährdet²⁰⁶ sehen.

Das Genehmigungssystem, das von Einzelgenehmigungen ausgeht, ver-
rät ein starkes Bestreben zum Schutz der Persönlichkeitsrechte des
Individuums, das jedoch auch protektionistischen oder sicherheitspoli-
tischen Charakter annehmen kann, vor allem bei der versuchten Er-

gänzung verknüpft werden können. Ausserdem wäre durch die
Verarbeitung der Daten im Ausland den schwedischen Behörden
die Vollzugs- und Durchsetzungsgewalt bei Zuwiderhandlungen
gegen die Bestimmungen des Datenschutzgesetzes verunmöglicht
worden (so die Begründung).

- Einer multinationalen Gesellschaft wurde mit der Entscheidung
vom 14.1.75 die Verlegung der Verarbeitung von Kundendaten der
schwedischen Zweigniederlassung nach England bewilligt, weil
die Zahl der in der Datenbank enthaltenen Personen sehr klein
war, kein allgemeines Personenkennzeichen (PIN = Personal Iden-
tification Number) zur Kombination mit bestehenden Datenbanken
verwendet wurde und die Datensicherheitsbestimmungen angemessen
waren. (Bemerkenswert ist, dass die Genehmigung trotz des
Fehlens eines Datenschutzgesetzes in England erteilt wurde.)
- Für Banken, die dem SWIFT-Netzwerk (vgl. vorne, S. 64ff.)
beitreten wollten, gab die schwedische Datenschutzbehörde im
Mai 1974 eine generelle Erlaubnis zum Export personenbezogener
Daten mittels des SWIFT-Netzes; auch Banken, die sich später
dem SWIFT-Netz anschlossen, wurde in einer Entscheidung vom
8.11.1976 in Anbetracht der grossen Sicherheitsvorkehrungen
und des geringen Risikos einer Persönlichkeitsverletzung der
Export von personenbezogenen Daten erlaubt.
- Im Zusammenhang mit einer Testinstallation auf einem neuen
Computersystem, das im Ausland installiert war, erteilte die
Datenschutzbehörde der gesuchstellenden Firma am 13. Okt.
1977, nach Ueberprüfung der Sicherheitsbestimmungen, eine auf
7 Wochen befristete Erlaubnis zum Export von Daten über mehr
als 2 Millionen Personen.

205 SARK, S. 9ff. und 18f.

206 STADLER, DSWR 4/76, S. 101.

haltung der staatlichen Unabhängigkeit z.B. gegenüber Ländern mit intensiver Informationstätigkeit. Hinsichtlich des anzustrebenden freien internationalen Datenaustausches unter den Staaten mit einem Datenschutzrecht ist aber dieser von der Erteilung einer Einzel- oder (in Ausnahmefällen) Mustergenehmigung abhängige Datenexport noch zu restriktiv geregelt. Auch wenn eine Genehmigung durch die Datenschutzbehörde regelmässig erteilt wird, falls im Staate des Empfängers ein dem schwedischen DSG entsprechendes Gesetz in Kraft steht, so vermag diese Regelung trotzdem nicht den Datenverarbeitern die notwendige Freizügigkeit bei der Verwendung personenbezogener Informationen im grenzüberschreitenden Datentransfer mit andern Datenschutzstaaten zu verschaffen.

Der Nachteil einer generellen Genehmigungspflicht im Verkehr mit Ländern mit Datenschutzgesetzen wird auch beim Zugriff von diesen Staaten aus auf schwedische Datenbanken ersichtlich. Hier werden innerhalb des Genehmigungssystems nur Mustergenehmigungen für den Zugriff auf bestimmte Datenarten opportun sein, da die Erteilung von Einzelgenehmigungen nicht praktikabel ist. Die Verpflichtung zur Einholung einer Genehmigung ist gegenüber Staaten mit vergleichbarer Gesetzgebung für Schweden wirtschaftlich von Nachteil, da diese Regelung den Aufbau von Verarbeitungssystemen mit multinationalen Datensammlungen über Personen hemmen kann.

b) Import personenbezogener Daten

Für den Import von Daten nach Schweden existieren keine besonderen Bestimmungen, so dass das Datenschutzgesetz in gleicher Weise auf Daten schwedischer wie ausländischer Staatsangehöriger, unabhängig von deren aktuellem Wohnsitz, anwendbar ist. Entscheidendes Kriterium für die Schutzwirkung des Gesetzes ist, dass die Verarbeitung der personenbezogenen Daten innerhalb des schwedischen Territoriums erfolgt. Geschützt sind somit die personenbezogenen Daten natürlicher Personen, die mit automatisierten Verarbeitungsmethoden im öffentlichen und privaten Bereich bearbeitet werden.

Der Import von Daten zum Vollzug eines speziellen Verarbeitungsvorganges innerhalb von Schweden ist unproblematisch zu bewerkstelligen, hingegen unterliegt der darauffolgende Export gemäss § 11 der Genehmigung durch die Datenschutzbehörde. Ob im Zusammenhang mit importierten Daten eine Mustergenehmigung²⁰⁷ für den Export erteilt wird, oder ob auch Einzelgenehmigungen erfolgen müssen, ist im Gesetz nicht geregelt - es liegt im Zuständigkeitsbereich der Datenschutzbehörde, dies festzusetzen. Hier wird auch die Haltung der Behörde bei der Erteilung von Exportgenehmigungen unterschiedlich sein,²⁰⁸ je nachdem, ob es sich bei den auszuführenden Daten um Angaben von nicht in Schweden wohnhaften, ausländischen Staatsangehörigen handelt oder um Daten schwedischer Bürger bzw. von Ausländern mit Wohnsitz in Schweden, die zwecks Durchführung bestimmter Verarbeitungsschritte nach Schweden importiert und anschliessend wieder ausgeführt werden sollen. Die Ausnützung spezialisierter, in Schweden befindlicher Computerkapazität durch verarbeitende Stellen mit Sitz in Ländern mit Datenschutzgesetzen wird aber durch eine Genehmigungsregelung zum Export der importierten Daten ungünstig beeinflusst. Diese Regelung verdeutlicht die Hindernisse, die beim "networking"²⁰⁹ auftauchen und dabei auch negativen Einfluss auf den Aufbau eines Netzwerkes ausüben können.

D. Frankreich

Die im französischen Datenschutzgesetz²¹⁰ verwirklichte Regelung des grenzüberschreitenden Datenverkehrs ist vor dem Hintergrund der auf dem institutionellen Modell²¹¹ basierenden Lösung zu betrachten.

207 Analog der Mustergenehmigung bei den SWIFT-Mitgliederbanken.

208 Dies ist aus den in der Kasuistik dargestellten Ueberlegungen ableitbar; vgl. vorne, S. 193, Anm. 203.

209 Vgl. vorne, S. 74.

210 Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIFL); französischer Originaltext in: Journal Officiel, 7.1.1978, S. 227ff.

211 Vgl. vorne, S. 189.

a) Export personenbezogener Daten

aa) Für den privaten Bereich

Die Ausfuhr von Daten ist grundsätzlich in Art. 24 LIFL geregelt, betrifft aber nach dem Wortlaut des Gesetzes nur die nicht öffentlichen Stellen.²¹² Der Wortlaut des Art. 24 reflektiert das institutionelle Modell und lautet:²¹³ "Auf Vorschlag oder gemäss einer Stellungnahme der Kommission kann die Uebermittlung personenbezogener Daten, die automatisch verarbeitet werden und unter die Regelung des Art. 16 fallen, aus dem französischen Hoheitsgebiet ins Ausland - in welcher Form auch immer sie durchgeführt wird - von einer vorhergehenden Erlaubnis abhängig gemacht oder gemäss von den durch Dekret des Staatsrates (Conseil d' Etat) festgelegten Modalitäten geregelt werden, um die Einhaltung der in diesem Gesetz festgelegten Prinzipien zu gewährleisten."²¹⁴ Daraus wird ersichtlich, dass das Gesetz selbst keine konkrete Regelung zum grenzüberschreitenden Datenverkehr abgibt, sondern die Ausgestaltung und Konkretisierung der Kommission oder dem Staatsrat überlässt. Die Datenschutzkommission²¹⁵ besitzt weitgehende Interpretations- und Ausgestaltungs-kompetenzen und hat ferner die Möglichkeit, dem Staatsrat den Erlass einer Verordnung vorzuschlagen, in der die Einzelheiten zum internationalen Datentransfer eine besondere Ausgestaltung innerhalb

212 Verweis auf Art. 16 LIFL, der eine negative Abgrenzung des privaten Bereiches gegenüber dem öffentlichen Sektor vornimmt.

213 "Sur proposition ou après avis de la commission, la transmission entre le territoire français et l' étranger, sous quelque forme que ce soit, d' informations nominatives faisant l' objet de traitements automatisés régis, par l' article 16 ci-dessus peut être soumise à autorisation préalable ou réglementée selon des modalités fixées par décret en Conseil d' Etat, en vue d' assurer le respect des principes posés par la présente loi."

214 BERHARD/GOLA/TUNER, DS+DS 3/78, S. 157.

215 Die "Commission Nationale de l' Informatique et des Libertés" (CNIL) setzt sich insgesamt aus 17 für eine Periode von 5 Jahren ernannten Mitgliedern zusammen.

dieses Bereiches erlangen.²¹⁶ Dies bedeutet, dass der Staatsrat - falls notwendig - durch ein Dekret eine neue Regelung zum grenzüberschreitenden Datenverkehr erlassen kann, die z.B. auf eine internationale Konvention abgestimmt ist. Die Flexibilität ist dabei optimal (Kommission oder Staatsrat können auch sofort auf Datenschutzgesetze anderer Länder Rücksicht nehmen und für diese einen genehmigungsfreien Export vorsehen), dafür leidet die Rechtssicherheit und Voraussehbarkeit - ein Mangel, der dem System des institutionellen Modells inhärent ist - bei der Beurteilung des Gesetzes, speziell aber durch das Ausland.

Grundsätzlich ist vorgesehen, den Export von personenbezogenen Informationen von einer Genehmigung der Datenschutzkommission abhängig zu machen; dabei wird bei der Erteilung von Genehmigungen die praktische Erfahrung bedeutenden Einfluss haben. Wann diese Genehmigung einzuholen ist, wird nirgends im Gesetz explizit ausgesagt - sie könnte bei der Anzeige der geplanten Datenverarbeitung vorgenommen werden, die nebst detaillierten Angaben zur Datenverarbeitung auch darüber Aufschluss geben muss, "ob die Datenverarbeitung für den Austausch personenbezogener Daten zwischen dem französischen Hoheitsgebiet und dem Ausland in irgendeiner Form bestimmt sind, auch wenn es um Massnahmen geht, die teilweise auf französischem Hoheitsgebiet auf der Grundlage von Massnahmen durchgeführt werden, die zuvor ausserhalb Frankreichs vollzogen wurden."²¹⁷ Wird die Genehmigung mit einer Bestätigung der Anzeige erteilt, die die Erlaubnis zum Beginn der Datenverarbeitung darstellt,²¹⁸ wird es sich vermutlich um eine Mustergenehmigung handeln. Ist die Genehmigung mit Angabe der not-

216 Die Kommission erstellt z.B. Gutachten oder unterbreitet dem Staatsrat Vorschläge, wenn der Export personenbezogener Daten ins Ausland einer Genehmigung unterworfen oder sonst in irgendeiner Weise geregelt werden soll, damit die Einhaltung des Gesetzes sichergestellt wird.

217 SCHOMERUS, DS+DS 2/78, S. 62; ferner Art. 19 LIFL.

218 Art. 16 LIFL.

wendigen Informationen anlässlich eines beabsichtigten Datenexportes einzuholen, ist sowohl eine Einzelerlaubnis wie Mustergenehmigung möglich. Der Charakter der Genehmigung ist im Gesetz nicht näher bestimmt und wird ebenfalls der Festsetzung durch die Kommission überlassen.

Nicht spezifisch geregelt ist die Frage, ob der direkte Zugriff vom Ausland auf Datenbanken mit personenbezogenen Informationen unter die Kategorie des Exportes fällt und damit ebenfalls einer Genehmigung unterliegt, oder ob diese Art von Datenausfuhr eine spezielle Ausgestaltung durch die Kommission erfährt.

Ausführungsbestimmungen haben auch darüber Aufschluss zu geben, ob die für den Export vorgesehene Genehmigung nur automationsunterstützt verarbeitete Angaben erfasst oder auch manuell erstellte Daten, die zur automatisierten Weiterverarbeitung ins Ausland übermittelt werden, sowie Computerausdrucke verarbeiteter Daten, die ebenfalls wieder erfasst und einer neuen Verarbeitung im Ausland unterzogen werden können.

Als Orientierungsmaßstab für die Erteilung einer Genehmigung oder der grundsätzlichen Erlaubnis zum Datenexport dienen die im LIFL verankerten Rechtsprinzipien: wird im Ausland die *ratio legis*, d.h. der Gedanke, dass die Datenverarbeitung allen Bürgern zu dienen hat und weder die menschliche Identität, noch die Grundrechte, noch das Privatleben, noch die individuellen und kollektiven Freiheitsrechte beeinträchtigen darf,²¹⁹ durch entsprechende Rechtsnormen beachtet, steht einem Export kein Hindernis entgegen. Somit besteht auch in Frankreich das Grundprinzip, dass für die Erteilung der Ausfuhrgenehmigung oder den (genehmigungs-)freien Export von Daten die Existenz einer vergleichbaren Gesetzgebung im Ausland zum Schutze der personenbezogenen Daten vorausgesetzt wird.

219 Vgl. Art. 1 LIFL und SCHINDEL, DSWR 10/78, S. 232.

bb) Für den öffentlichen Bereich

Das Gesetz schliesst die Anwendung des Art. 24²²⁰ für den öffentlichen Bereich aus, regelt aber nirgends ausdrücklich den von Behörden und anderen öffentlichen Stellen durchzuführenden Export personenbezogener Daten (z.B. im Zusammenhang mit dem behördlichen Austausch personenbezogener Informationen innerhalb der EG). Da im öffentlichen Sektor die Datenverarbeitung gemäss Art. 15 Abs 1 LIFL nur zulässig ist, soweit sie "nach begründeter Stellungnahme der Kommission, durch Gesetz oder verwaltungsrechtlich bestimmt ist",^{221 222} muss der gesetzlichen oder verwaltungs- bzw. verordnungsrechtlichen Grundlage entnommen werden, ob im Aufgabenbereich der (die obrigkeitliche Tätigkeit ausführenden) Behörde der Export von Daten miteinbezogen ist oder nicht. Gehört die Datenausfuhr in den gesetzlich oder verordnungsrechtlich umschriebenen Wirkungsbereich der die Verarbeitung durchführenden öffentlichen Stelle, ist mit der Genehmigung der Verarbeitung als solcher - mangels anderer Vorschrift - auch eine konkludente Einwilligung der Kommission zum Export der personenbezogenen Informationen anzunehmen.²²³ Dies ist die logische Konsequenz einer positiven Stellungnahme der Kommission, welcher bei einer potentiellen Gefährdung des Gesetzeszweckes auch eine negative Bescheiderteilung offenstehen würde.

cc) Für beide Bereiche geltende Bestimmungen

Art. 37 schreibt vor, dass eine Datensammlung mit personenbezogenen Informationen von Amtes wegen ergänzt oder berichtigt werden muss, wenn die Stelle, die sie unterhält, Kenntnis von der Unrichtigkeit oder Unvollständigkeit der in dieser Datenbank enthaltenen Angaben erhält. Diese Vorschrift erlangt auch für den internationalen Datenaustausch, insbesondere für den Export von Daten im Zusammenhang mit Art. 38 LIFL Bedeutung.

220 Vgl. vorne, S. 197.

221 SCHINDEL, DSWR 10/78, S. 233.

222 Legalitätsprinzip.

223 HOLLEAUX, S. 37, N V.

Art. 38 verpflichtet denjenigen, der die Daten an einen Dritten übermittelt hat, eine Berichtigung oder Annullierung der Angaben dem Empfänger mitzuteilen, falls die Kommission ihn nicht von dieser Pflicht entbunden hat.

Auch hier ist es möglich, beim Export von Daten dem inländischen Absender die Pflicht zur Weiterleitung der Berichtigungen und Ergänzungen aufzuerlegen; sie trifft aber nur den in Frankreich befindlichen Datenverarbeiter oder Datenbankhalter. Die im Ausland lokalisierte Stelle, die diese Daten aus Frankreich empfängt, ist - sofern das auf sie anwendbare Datenschutzgesetz dies nicht vorschreibt - weder verpflichtet, i.S. von Art. 37 LIFL eine Korrektur bzw. Ergänzung oder Löschung dieser Daten vorzunehmen, noch solche Ergänzungs- bzw. Korrekturmeldungen weiterzuleiten, falls die Daten bereits verarbeitet und an eine weitere Stelle ins Ausland übermittelt wurden. Hier wird wiederum der enge Geltungsrahmen eines nationalen Gesetzes deutlich, dessen Schutzfunktionen durchbrochen werden können, sobald die personenbezogenen Informationen seinen Geltungsbereich verlassen; an diesem Punkt hat eine internationale Konvention anzusetzen und den national beschränkten Anwendungsbereich mittels entsprechender Vorschriften auszudehnen, um den Schutzansprüchen der nationalen Datenschutzgesetze auf internationaler Basis zum Durchbruch zu verhelfen.

Die Ausgestaltung der Regelung von Art. 38 wird der Kommission überlassen, welche einer exportierenden Stelle die Pflicht zur Weiterleitung der Berichtigung und Ergänzung vorschreiben oder sie davon entbinden kann. Solange aber im Empfängerland keine analoge oder ähnliche Pflicht zur Korrektur besteht, wird die vom LIFL beabsichtigte Wirkung an der fehlenden Durchsetzbarkeit im Ausland scheitern.

Wenn Datenschutz verwirklicht werden soll, dürfen die Vorschriften von Art. 37 und 38 LIFL nicht als sinnlos taxiert werden, auch wenn ihre Verwirklichung im Ausland nicht sichergestellt ist, weil die Aktualität der Angaben einer der wichtigsten Faktoren des Datenschutzes schlechthin darstellt und einen entsprechenden Stellenwert im nationalen wie auch im internationalen Informationsverkehr hat.²²⁴

b) Import personenbezogener Daten

Das französische Datenschutzgesetz enthält keine besonderen Bestimmungen, die den Import von Daten regeln. Die Anwendbarkeit des Gesetzes erstreckt sich auf alle in Frankreich bzw. im französischen Hoheitsbereich lokalisierten Datenverarbeitungsanlagen und die damit durchgeführten Verarbeitungsschritte personenbezogener Daten natürlicher Personen.²²⁵ Aus dem Gesetzeswortlaut ist keine unterschiedliche Behandlung der französischen und ausländischen Staatsangehörigen ersichtlich, so dass dem Prinzip der Gleichbehandlung Genüge getan ist.

Der Import von Daten zum Vollzug eines oder mehrerer Datenverarbeitungsschritte in Frankreich durch einen dem privaten Bereich angehörenden Rechtsträger ist problemlos möglich, sofern die Durchführung der Verarbeitung die Erfordernisse des Gesetzes erfüllt (Art. 16 LIFL). Die Wiederausfuhr dieser importierten Daten wird aber im privaten Bereich von den Ausführungsbestimmungen der Kommission abhängig sein, die dafür eine Genehmigung zur Ausfuhr vorsehen, aber auch darauf verzichten kann.

Vollzieht eine staatliche Stelle, eine öffentliche Anstalt, eine Gebietskörperschaft oder eine mit öffentlichen Aufgaben betraute private Stelle den Import personenbezogener Daten, müssen diese Vorgänge nach dem Legalitätsprinzip ebenfalls auf gesetzlicher oder verordnungsrechtlicher Grundlage beruhen, die ihrerseits durch die behördliche Genehmigung zur Datenverarbeitung mitabgedeckt sein muss.

-
- 224 Damit ist aber das Problem der Nachführung und Berichtigung von international übermittelten Daten noch keineswegs gelöst. Es ist möglich, dass eine solche Regelung auf internationaler Basis die datenverarbeitenden Stellen vor unüberbrückbare Probleme stellt, weil sie z.T. in einem erheblichen Kostenaufwand resultieren, so dass u.U. eine begrenzte Speicherdauer für ins Ausland übermittelte Daten eine günstigere Lösung darstellen kann (nach Ablauf dieser Dauer müssten die Daten neu beschafft werden).
- 225 Das LIFL schützt nicht personenbezogene Daten juristischer Personen.

E. Dänemark

Das dänische Datenschutzrecht wird von zwei Gesetzeswerken gebildet, die getrennt den privaten²²⁶ und öffentlichen²²⁷ Bereich abdecken.

a) Export personenbezogener Daten

aa) Gesetz über private Register

Das Gesetz enthält in § 21 Bestimmungen zur Datenverarbeitung ausserhalb Dänemarks; dabei wird unterschieden zwischen der Speicherung von Daten für ausländische Systeme und der Uebermittlung zur Datenverarbeitung im Ausland.

Bei der Speicherung von Daten ausserhalb Dänemarks erfahren drei unterschiedliche Datengruppen eine differenzierte Regelung:

- Zur Verhinderung der Umgehung des Datenschutzgesetzes wird als erstes bestimmt, dass Daten, die in Dänemark nicht gespeichert und verarbeitet werden dürfen (z.B. sensitive Daten²²⁸), auch nicht ausserhalb des Landes zu Speicherungszwecken gesammelt werden dürfen.²²⁹
- Die Daten, die im Inland der Registrierungs- oder Anzeigepflicht an die Datenschutzbehörde unterliegen, bedürfen zur Speicherung im Ausland einer Genehmigung durch diese Behörde.
- Alle übrigen Daten, für die keine spezielle Registrierungspflicht vorgeschrieben ist, dürfen frei im Ausland gespeichert werden.²³⁰

Bei der Uebermittlung personenbezogener Angaben zur automationsunterstützten Verarbeitung im Ausland unterliegen nur die sensitiven

226 Gesetz über private Register Nr. 293 vom 8.6.1978: Lov om private registre, No. 293.

227 Gesetz über Register bei öffentlichen Stellen Nr. 294 vom 8.6.1978: Lov om offentlige myndigheders m.v., No. 294.

228 Daten über Rasse, religiöse Ueberzeugung, politische Ansichten etc., vgl. § 3.

229 Diese Vorschrift ist aber nur an die Normadressaten, d.h. die innerhalb des Geltungsbereiches vom Gesetz erfassten Datenverarbeiter gerichtet (Territorialitätsprinzip).

230 § 21 Abs. 1.

Daten i.S. von § 3 Abs. 2 einer Genehmigung durch die Datenschutzbehörde. Eine Erlaubnis durch die Datenschutzbehörde ist ebenfalls erforderlich für das systematische Sammeln sensibler Daten, das im Hinblick auf eine elektronische Verarbeitung ausserhalb Dänemarks erfolgt.^{231 232}

Eine Ausnahme zu dieser Bestimmung existiert für diejenigen Systeme, die ausschliesslich dem Vollzug einzelner Verarbeitungsvorgänge innerhalb Dänemarks dienen.²³³ Diese Uebermittlungen bedürfen keiner Exportgenehmigung, auch wenn sie sensitive Informationen beinhalten. Dies bedeutet, dass eine nicht dänische Gesellschaft, die im Rahmen ihrer Verarbeitungstätigkeit in Dänemark lokalisierte Datenverarbeitungssysteme benutzt und dabei Daten nur zur Ausführung eines einzelnen oder mehrerer Vorgänge auf dieses System in Dänemark importiert, diese Angaben ohne Genehmigung der Datenschutzbehörde wieder exportieren kann, ungeachtet dessen, ob die ein- und ausgeführten Daten nach dänischem Recht als sensitiv zu qualifizieren waren oder nicht.²³⁴ Damit nimmt das Gesetz explizit zur Frage des Exportes von zu speziellen Verarbeitungsvorgängen nach Dänemark importierten Daten Stellung und erlaubt eine sehr freie Handhabung dieses Bereiches.

Nach § 21 Abs. 3 ist für die Erteilung von Genehmigungen durch die Datenschutzbehörde massgeblich, dass durch die Uebermittlung bzw. Speicherung im Ausland keine Schwächung oder Vereitelung des vom Gesetz bezweckten Schutzes der Daten herbeigeführt wird. Eine Genehmigung zum Export wird m.a.W. ausgesprochen, wenn im Destinationsland ein ausreichender Datenschutz verwirklicht ist.²³⁵ Nach Abs. 4 besteht sogar die Möglichkeit, im Hinblick auf internationale Verträge oder internationale Zusammenarbeit gewisse Erleichterungen einzuräumen, falls in Vertragsländern ein vergleichbarer oder gleichwertiger

231 § 21 Abs. 2.

232 BURKERT/ENGEL, DS+DS 1/80, S. 51.

233 § 21 Abs. 2 Satz 3.

234 TDR, Vol. 1, No. 4, August 1978, S. 8.

235 Vgl. auch 1. Tätigkeitsbericht d.B.f.D., S. 59.

Datenschutz realisiert ist und keine Verminderung des Schutzzweckes dieses Gesetzes befürchtet werden muss (Prinzip der Gegenseitigkeit).

Ausserdem enthält § 20 Abs. 2, der bereichsspezifisch die Verarbeitungsmodalitäten für die Service-Rechenzentren regelt, die Vorschrift, dass diese nicht ohne Genehmigung des Besitzers des Registers bzw. des Auftraggebers die Daten im Ausland speichern dürfen.

Aehnlich wie in Frankreich²³⁶ kann die dänische Datenschutzbehörde die datenverarbeitenden Stellen verpflichten, die Empfänger (Dritte) aller während der letzten sechs Monate weitergegebenen Daten über eine Vernichtung, Ergänzung oder Korrektur zu benachrichtigen. Diese Verpflichtung kann auch internationale Dimensionen annehmen, wenn sie einer Gesellschaft auferlegt wird, die innerhalb der letzten sechs Monate Daten an Dritte im Ausland übermittelt hat.

§ 7 dehnt den Geltungsbereich des Gesetzes aus auf Daten, die ausserhalb des dänischen Hoheitsbereiches verarbeitet werden, d.h. die im Ausland verarbeiteten Daten unterliegen gemäss § 6 Abs. 1 der Löschung, sobald sie ihre Relevanz für die ursprüngliche Zweckbestimmung verloren haben; nach Abs. 2 trifft das verarbeitende Unternehmen eine Aktualisierungspflicht sowie die Einführung von Kontroll- und Sicherheitsmassnahmen.²³⁷ Nach Ansicht der dänischen Expertenkommission ist es Sache der Unternehmen, die ausländische Computer benutzen, darum besorgt zu sein, dass die Massnahmen des Gesetzes befolgt werden. M.E. sind solche Vorschriften wenig wirksam, da die Durchsetzbarkeit fehlt - effizienter wäre es, die Zulässigkeit der Datenverarbeitung von der Beachtung entsprechender Sicherheitsvor-

236 In Frankreich besteht die Pflicht zur Benachrichtigung von Gesetzes wegen und beschränkt sich nicht auf die während der letzten sechs Monate übermittelten Daten.

237 Die Anwendung dieser Verpflichtung ist aber nur in denjenigen Fällen sinnvoll, wo eine Inlandsbeziehung vorhanden ist, sei es dass die Daten eine in Dänemark wohnhafte Person betreffen oder von einem dänischen Unternehmen durchgeführt werden.

kehrungen abhängig zu machen und mittels einer gesetzlichen Vorschrift der Nachführung, Ergänzung und Vernichtung von ins Ausland transferierten Daten Nachdruck zu verleihen. Der Vollzug solcher nationaler Vorschriften beim Datenempfänger im Ausland ist aber ohne korrespondierende ausländische Vorschrift oder völkerrechtliche Verträge nicht durchsetzbar.

bb) Gesetz über öffentliche Register

Das Gesetz über öffentliche Register enthält keine speziellen Vorschriften zum Export personenbezogener Daten staatlicher oder kommunaler Behörden an eine öffentliche oder private Stelle im Ausland. Es existieren lediglich die Bestimmungen über die Zulässigkeit der Uebermittlung an Private und an andere öffentliche Stellen im Inland. Eine Anwendung dieser Bestimmungen auf eine Uebermittlung ins Ausland scheint mangels gegenteiliger Vorschrift und unter Beachtung des Legalitätsprinzips als zulässig.

Materiell ist eine Uebermittlung von Daten des öffentlichen Sektors grundsätzlich nicht erlaubt;²³⁸ in drei Ausnahmefällen ist jedoch eine Uebermittlung gestattet

- wenn die Öffentlichkeit bereits Zugang zu den Daten hat;
- bei schriftlicher Zustimmung des Betroffenen zur Uebermittlung der Daten;
- bei Erfüllung der Bedingungen der §§ 17 - 19.²³⁹

Für die Uebertragung von Daten innerhalb des öffentlichen Bereichs gelten die gleichen Zulässigkeitsvoraussetzungen wie für den

238 BURKERT/ENGEL, a.a.O., S. 47; TDR, Vol. 1, No. 4, S. 8.

239 - Nach § 17, wenn der Private für öffentliche Behörden Aufgaben erfüllt und an eine identische Zweckbestimmung gebunden ist.
- Nach § 18, für medizinische Daten, wobei entweder konkludente Zustimmung der betroffenen Individuen oder Zustimmung des Gesundheitsministeriums oder der Datenschutzbehörde (z.B. bei Uebermittlung in Register, die nicht in den Anwendungsbereich des Gesetzes über öffentliche Register fallen) gegeben sein muss.

privaten Sektor; ausserdem ist sie aber auch gestattet, wenn die empfangende Stelle von Gesetzes wegen Zugang zu diesen Daten hat oder die andere öffentliche Stelle die Daten zur gesetzlich festgelegten Aufgabenerfüllung benötigt. Bei einem Export der Daten an eine öffentliche Behörde im Ausland müsste demnach die festgelegte Aufgabenerfüllung entweder auf Gesetz oder einem völkerrechtlichen Vertrag beruhen.

Da die staatlichen oder kommunalen datenverarbeitenden Stellen an das Legalitätsprinzip gebunden sind, und die Datenschutzbehörde bei der Errichtung der Datenverarbeitungsanlagen mitwirkt, ist eine Beachtung des vom Gesetz beabsichtigten Schutzzweckes sichergestellt - im Zweifelsfall ist die Datenschutzbehörde um Rat bzw. um eine Genehmigung anzugehen.

b) Import

Keines der beiden Datenschutzgesetze enthält spezielle Bestimmungen zur Einfuhr von personenbezogenen Angaben, weil sie automatisch unter den Anwendungsbereich des dänischen Datenschutzrechts fallen, sobald sie auf einem im Inland lokalisierten Datenverarbeitungssystem automationsunterstützt verarbeitet werden. Eine Unterscheidung der Daten nach dem Wohnsitz oder der Staatsangehörigkeit des Datensubjekts existiert nicht, so dass die aus der Verarbeitung fliessenden Individualrechte jedem Betroffenen zustehen.

c) Folgerung

Die im Gesetz für die privaten Register getroffene Regelung der grenzüberschreitenden Informationsverarbeitung ist eher restriktiver Natur. Die Differenzierung zwischen einer Sammlung personenbezogener dänischer Angaben für deren Einbeziehung (Speicherung) in einem ausländischen Datenverarbeitungssystem und dem Export gespeicherter In-

- Nach § 19, wenn ein rechtliches Interesse an den Einzeldaten das Geheimhaltungsinteresse deutlich überwiegt (BURKERT/ENGEL, a.a.O., S. 48).

formationen zur Datenverarbeitung im Ausland ist nicht in allen Fällen einfach zu vollziehen,²⁴⁰ bietet aber die Möglichkeit, den unterschiedlichen Gefahren mit einer abgestuften Genehmigungsregelung zu begegnen.

M.E. kann der genehmigungsfreie Export von personenbezogenen Daten zur Verarbeitung im Ausland i.S. von § 21 Abs. 2 des Gesetzes über private Register trotz der Vorschrift von § 7 zu Missbräuchen Anlass geben, so dass hier mit der Beschränkung der Genehmigung auf die sensitiven Daten noch eine Gesetzeslücke besteht (freilich nur gegenüber Ländern, die über keine vergleichbare Datenschutzgesetzgebung verfügen).

Begrüssenswert ist der erleichterte Transfer bzw. die genehmigungsfreie Ausfuhr von Daten, die lediglich zwecks Benutzung bestimmter dänischer Hard- und Software-Kapazität zur Verarbeitung eingeführt und wieder exportiert werden. Diese Regelung trägt dem Umstand Rechnung, dass bei blossem Gebrauch fremder Computerkapazität häufig keine Kombination mit personenbezogenen Angaben aus dem gespeicherten Datenbestand des benutzten Systems erfolgt.

Vermisst wird hingegen eine spezifische Norm zum grenzüberschreitenden Datenverkehr im Gesetz über öffentliche Register. Obwohl auch im dänischen Datenschutzrecht die Verarbeitung von Daten im öffentlichen Bereich nach dem Grundsatz der Gesetzmässigkeit der Verwaltung auszuführen ist, wird es angesichts unklarer Verhältnisse am einfachsten sein, die dänische Datenschutzbehörde anzufragen, um über die Zulässigkeitsvoraussetzungen zum Export verbindliche Aussagen zu erhalten: ein Weg, der das Erfordernis der Voraussehbarkeit durch ausländische öffentliche und private Rechtsträger keineswegs berücksichtigt. Diese Tatsache ist umso bedauernswerter, als innerhalb der EG ein verstärkter Austausch personenbezogener Daten zwischen öffentlichen Stellen stattfindet und zukünftig in noch ausgedehnterem Umfang durchgeführt werden dürfte.

240 Hier haben Praxis und Doktrin klare Abgrenzungskriterien zu definieren.

F. Norwegen

Das norwegische Datenschutzgesetz ²⁴¹ enthält im 9. Kapitel mit den §§ 36 und 37 spezielle, für den grenzüberschreitenden Datenverkehr zugeschnittene Normen.

a) Export personenbezogener Daten

Bezugspunkt der in § 36 festgelegten Ordnung zur Ausfuhr von Informationen bildet § 9, der sowohl für die elektronische als auch manuelle Verarbeitung von Daten eine Bewilligungspflicht vorsieht; für die manuell geführten Datensammlungen allerdings nur, falls sie sensitive Angaben ²⁴² enthalten. Daraus ergeben sich zwei Arten von Datensammlungen, welche zur Verarbeitung einer Bewilligung bedürfen:

- Datenregister, die elektronisch verarbeitet werden bzw. worden sind, und
- manuell bearbeitete Datensammlungen, die sensitive Informationen enthalten.

Für den Export von Daten aus diesen Registern ist in § 36 Abs.1 eine Genehmigung durch den König ²⁴³ vorgeschrieben, alle übrigen Datenarten und Sammlungen ²⁴⁴ können ohne Einschränkungen exportiert werden. Die Bewilligungspflicht für die Verarbeitung im Inland ist ausschlaggebend für die Genehmigungspflicht zum Export.

Ausserdem wird in § 36 Abs.2 eine weitere Unterscheidung vorgenommen: Die Weitergabe personenbezogener Informationen, die innerhalb des norwegischen Gebietes erhoben und gesammelt werden, um in Datensammlungen ²⁴⁵ ausserhalb Norwegens gespeichert zu werden, darf nur

241 Lov nr. 48 om personregistre m.m. av. 9 juni 1978.

242 Angaben über rassische Zugehörigkeit, politische oder religiöse Ansichten, Vorstrafen, Gesundheit, Drogenmissbrauch, Sexualleben und familiäre Verhältnisse (vgl. § 9 Abs. 1 Ziff. 1-5).

243 Bzw. Regierung.

244 Z.B. manuelle mit personenbezogenen Angaben, die keinen sensitiven Charakter haben.

245 Datensammlungen, die ebenfalls entsprechend den in § 9 aufgezählten Kriterien einer Genehmigungspflicht unterliegen.

mit einer speziellen Genehmigung des Königs bzw. der Regierung erfolgen. Damit deckt das Gesetz einen aus der Beschränkung auf automatisierte Bearbeitungsvorgänge resultierenden unklaren Bereich der Verarbeitungsphasen ab.²⁴⁶

Abs. 3 statuiert eine Ausnahme von der Bewilligungspflicht durch Entscheid des Königs bzw. der Regierung "für die Fälle, wo für den Export in bestimmte Länder keine Erlaubnis vorgeschrieben werden soll."²⁴⁷ Diese Ausnahmebestimmung betrifft die Exporte in Länder mit eigener Datenschutzgesetzgebung, so dass auch hier ein möglichst freier und ungehinderter Datenaustausch unter "Datenschutz-Staaten" als Zielprojektion der gesetzlichen Regelung des grenzüberschreitenden Datentransfers erscheint.

b) Datenimport

Zum Datenimport enthält das Gesetz keine spezifischen Bestimmungen: Die importierten Daten, die in Norwegen verarbeitet und gespeichert werden, unterliegen dem Anwendungsbereich des Gesetzes, das keinen Unterschied zwischen den Daten bezüglich ihrer territorialen Provenienz macht.

c) Spezielle Norm für internationale Aktivitäten

§ 37 bezieht sich ebenfalls auf den Datenverkehr mit dem Ausland und gibt dem König bzw. der Regierung die Befugnis, Bestimmungen über die Zusammenarbeit des norwegischen Datenüberwachungsdienstes mit ausländischen Datenschutzbehörden zu erlassen. Das Gesetz nennt als möglichen Inhalt solcher Verordnungen spezielle Vorschriften bezüglich der Bewilligungspflicht für Datenregister sowie für die Ueberwachung oder Löschung von Datensammlungen. Diese Norm gibt dem König bzw. der Regierung die Kompetenz, nicht nur für die zwischenstaatliche Zusammenarbeit, sondern auch für eine norwegische Beteiligung an internationalen Vereinbarungen zum grenzüberschreitenden Datenverkehr spezielle Normen zu erlassen. Damit hält sich das norwegische Daten-

²⁴⁶ Vgl. nachfolgend d), S. 211.

²⁴⁷ BURKERT/ENGEL/JOHNSEN, DS+DS 4/79, S. 256.

schutzgesetz die Möglichkeit offen, auf zwischenstaatliche²⁴⁸ und internationale Uebereinkommen zum internationalen Datenverkehr zweckmässig zu reagieren und zu solchen Vereinbarungen entsprechende Anpassungsbestimmungen für das nationale Gesetz zu erlassen: eine weitsichtige Lösung, deren Flexibilität im institutionellen Modell begründet ist.

d) Folgerung

Gegenüber den in andern Ländern²⁴⁹ herrschenden Regelungen ist auf die Anwendung der Bestimmungen über Datenexport sowohl auf die für den Export vorgesehenen, gespeicherten personenbezogenen Angaben bzw. Sammlungen als auch auf die im Inland erhobenen aber zur Speicherung im Ausland bestimmten Daten hinzuweisen. Sie dient dazu, eine Unklarheit des Gesetzes zu beseitigen, die wegen des auf die automationsunterstützte Verarbeitung beschränkten Geltungsbereiches auftritt, und unterstellt deshalb jede Weitergabe von geschützten Daten ins Ausland einer Genehmigungspflicht. Diese Differenzierung ist in all jenen Fällen zu begrüßen, in denen der Datenschutz auf die automatisierten Bearbeitungsvorgänge beschränkt ist und die manuellen Verarbeitungsschritte in die automationsunterstützten Abläufe miteinbezogen sind.²⁵⁰ Damit wird eine Umgehung des Gesetzes über manuell zu vollziehende Phasen vermieden.

Eine vollständige Beurteilung der auf Datenexporte anwendbaren Vorschriften setzt allerdings die Kenntnis der jeweils in Kraft stehenden Ausnahmebestimmungen in Verordnungen voraus, so dass für die Empfänger exportierter Daten eine Kontaktaufnahme mit der Datenüberwachungsbehörde empfehlenswert erscheint.

248 Z.B. im nordischen Rat verabschiedete Vereinbarungen.

249 Ausnahme: Dänemark: § 21 Abs.2 Satz 2 (aber nur hinsichtlich sensitiven Daten): vgl. vorne, S. 204, Anm. 231.

250 Wie z.B. in Oesterreich; vgl. vorne, S. 186f.

G. Luxemburg

Im luxemburgischen Datenschutzgesetz²⁵¹ existieren mehrere Bestimmungen, die nebst der Regelung der inländischen Datenverarbeitung auch spezielle Anordnungen für den grenzüberschreitenden Datenverkehr enthalten; ein eigentlicher, umfassender Abschnitt zu diesem Themenkreis fehlt aber im luxemburgischen Gesetzeswerk.

a) Export personenbezogener Daten

Das Gesetz enthält keine spezifischen materiellen oder formellen Bestimmungen zum Datenexport. Die einzige Norm im Zusammenhang mit der Ausfuhr von Daten ist Art. 3 Abs. 2 Satz 1 und betrifft den Anwendungsbereich des Gesetzes. Nach dieser Bestimmung sind die Vorschriften des Gesetzes auf alle in Luxemburg errichteten Datenbanken anwendbar, auch wenn die Daten ausschliesslich im Ausland benutzt werden.

Diese allgemeine Formulierung lässt verschiedene Interpretationen zu und bedarf hinsichtlich ihrer Tragweite für die Ausfuhr personenbezogener Daten dringend einer Begriffsbestimmung durch Doktrin und Praxis. So ist m.E. mit dieser Norm gleichzeitig eine Ausdehnung des Anwendungsbereiches auf das Ausland gegeben und zwar in dem Sinne, dass dem nicht in Luxemburg befindlichen Benutzer eines Terminals die im luxemburgischen Gesetz formulierten Vorschriften beim Umgang mit den luxemburgischen Daten zur Beachtung auferlegt werden.²⁵² Bestimmungen dieser Natur sind aber wenig geeignet, die rechtlichen Regeln des internationalen Datenverkehrs übersichtlich

251 Loi du 31 mars 1979 réglementant l' utilisation des données nominatives dans les traitements informatiques (veröffentlicht im Amtsblatt des Grossherzogtums Luxemburg Nr. 29 vom 11. April 1979, S. 581ff.); vgl. in diesem Zusammenhang auch loi du 30 mars 1979 organisant l' identification numérique des personnes physiques et morales (Personenkennzeichen).

252 Gl.M. STADLER, OeVD 10/79, S. 10: "... das Bemühen um eine Ausweitung des Geltungsbereiches auf alle Datenbanken, die einen auch nur durch Terminals gegebenen Konnex zum luxemburgischen Staatsgebiet haben."

und einfach zu gestalten: einerseits fehlt den nationalen Vorschriften ausserhalb des territorialen Anwendungsbereiches die Durchsetzbarkeit und andererseits können sie beim Normadressaten Zielkonflikte²⁵³ erzeugen und damit die Rechtssicherheit ganz allgemein beeinträchtigen.

Die Regelung erwähnt nur die Benützung im Inland (Luxemburg) liegender Datenbanken durch Stellen im Ausland. Dabei bleibt unklar, was der Begriff der "Benützung von Daten einer in Luxemburg liegenden Datenbank" beinhaltet. Naheliegend^{254 255} ist, dass der Gesetzgeber damit den Zugriff auf die in Luxemburg befindlichen Datenbanken mittels im Ausland gelegener Terminals²⁵⁶ meint; ob er darunter aber auch den Export von Angaben aus 'luxemburgischen' Datenbanken in Datensammlungen des Auslandes versteht, ist dem Wortlaut des Gesetzes nicht schlüssig zu entnehmen, da konkrete Anhaltspunkte fehlen. Der substantielle Unterschied dieser beiden Varianten des Datenexportes wird dadurch deutlich, dass beim Zugriff auf Datenbanken vom Ausland in der Regel²⁵⁷ keine physische Verschiebung des Speicherortes durch eine Uebertragung der Daten auf das ausländische Datenverarbeitungssystem stattfindet, sondern nur ein Datentransfer zwischen Datenspeicher bzw. Computer und Datenstation erfolgt, während beim Export von Daten eine Uebermittlung personenbezogener Daten aus den Dateien luxemburgischer Datenverarbeitungssysteme in die Datenbestände eines ausländischen Computersystems vollzogen wird, wodurch die Übermittel-

253 Ein Zielkonflikt kann dadurch entstehen, dass der Normadressat einerseits das nationale Gesetz befolgen und andererseits auch noch ein davon abweichendes ausländisches Recht (das seinen Geltungsbereich ausdehnt) beachten sollte.

254 Vgl. TDR, Vol. 2, No. 1, 1979, S. 2; STADLER, OeVD 10/79, S. 8 und v.a. 10.

255 Das Wort 'Terminal' wird im folgenden Satz für den umgekehrten Fall des Datenimportes im Gesetzestext verwendet (vgl. hinten, S. 215, Anm. 266).

256 M.a.W.: Datenstation.

257 Nicht ausschliesslich, denn technisch ist eine Uebernahme der Daten auf ein am Terminal angeschlossenes, ebenfalls im Ausland gelegenes Datenverarbeitungssystem möglich.

ten Daten in bestehende oder neu geschaffene Dateien integriert werden, was wiederum eine selektive²⁵⁸ oder konsolidierte²⁵⁹ Verarbeitungs- und Auswertungsmöglichkeit gestattet.

Es ist aber auch denkbar, dass die entsprechenden nationalen Bestimmungen betreffend die Datenübermittlung ohne spezielle Differenzierung²⁶⁰ auch für die Exporte ins Ausland anwendbar sein sollen. Die Konsequenz einer solchen Lösung würde darin bestehen, dass der Besitzer oder Führer einer privaten oder öffentlichen²⁶¹ Datensammlung beim Antrag auf Zulassung der Datenverarbeitung in den von Art. 5 Abs. 3 lit. e geforderten Detailangaben die Natur der ins Ausland zu übermittelnden Daten, die transferierten Ergebnisse sowie den oder die Empfänger im Ausland zu deklarieren hätte, so dass aufgrund dieser Angaben der Antrag auf Bewilligung vom zuständigen Minister geprüft werden kann. Mit der Genehmigung des Antrages auf Zulassung der Datenbank würde auch der deklarierte Export personenbezogener Daten an den oder die aufgeführten Empfänger im Ausland erlaubt. Jede Aenderung der einer Genehmigung zugrundeliegenden Umstände bedarf nach Art. 6 einer neuen Bewilligung der Datensammlung durch den Minister, somit auch jede Ergänzung oder Aenderung der Empfänger von Uebermittlungen im Ausland, so dass der positive oder negative Entscheid über die Zulassung einer Datenbank u.U. von einem im Ausland befindlichen Empfänger abhängig sein kann.²⁶² Eine solche Zulassung kommt durch

258 Z.B. nur luxemburgische Daten allein.

259 Luxemburgische Informationen, gemischt mit Daten anderer Provenienz.

260 Vgl. BDSG, das die Zulässigkeitsvoraussetzungen der Uebermittlungen im Inland auch für den Fall der Uebermittlung ins Ausland vorsieht.

261 Satz 2 von Art. 9 verweist für die Errichtung öffentlicher Datenbanken auf Art. 5 Abs. 3.

262 Ein negativer Entscheid muss entsprechend Art. 6 begründet werden, so dass ersichtlich wird, ob der ausländische Destinatär Ursache der Verweigerung der Genehmigung ist, weil Grund zur Annahme besteht, dass die Daten missbräuchlich oder entgegen den gesetzlichen Bestimmungen verwendet werden (STADLER, OeVD 10/79, S. 8).

die Deklarationspflicht der auszuführenden Daten einer (Muster-) Genehmigung zum Export bestimmter Daten an die angegebenen Empfänger gleich. Mithin gewährt die Durchführung dieses Zulassungsverfahrens die behördliche Durchgriffsmöglichkeit im Falle von Gesetzesverletzungen.²⁶³ In diesem Zusammenhang ist auch Art. 23 bedeutsam, der - analog zu Frankreich²⁶⁴ - bei Uebermittlungen vorschreibt, dass Korrekturen und Löschungen von Daten den Drittempfängern mitgeteilt werden müssen.

b) Import personenbezogener Daten

Im Gegensatz zu andern Datenschutzgesetzen behandelt das luxemburgische Datengesetz den Import personenbezogener Informationen ausführlicher und umfassender. Es ergeben sich hier, anders als beim Export, weniger ungeklärte Fragen, da die Regelung auf dem Territorialprinzip beruht.

Art. 3 Abs. 2 Satz 2²⁶⁵ umreißt den Anwendungsbereich des Gesetzes für den Fall, dass von luxemburgischen Gebiet auf eine im Ausland errichtete Datenbank mittels Terminal zugegriffen wird: der Benutzer dieser Datenstation in Luxemburg hat die Bestimmungen des Gesetzes zu beachten. Die über diese Datenstation importierten ausländischen Daten unterstehen damit dem Schutzbereich des luxemburgischen Gesetzes, da für den luxemburgischen Benutzer der eingeführten Daten die lex fori massgeblich ist.

Wie beim Export²⁶⁶ erwähnt das Gesetz nur den Fall der Einfuhr mittels Terminals, aber nicht die Variante einer Computerverbindung bzw. Import von im Ausland erhobenen Daten zur Bearbeitung in Luxemburg. Es ist Sache der Lehre sowie der zuständigen Organe, eine Klärung dieser Frage vorzunehmen und den genauen Begriffsinhalt festzulegen.

263 STADLER, OeVD 10/79, S. 9.

264 Vgl. vorne, cc), S. 200f.

265 Umgekehrter Fall von Satz 1 (vgl. vorne, S. 212).

266 Vgl. vorne, S. 213f.

Der auf luxemburgischen Gebiet befindliche Benutzer hat für den Zugriff auf und die Nutzung von Datenbanken, die ausserhalb Luxemburgs liegen, gemäss Art. 5 Abs. 2 ebenfalls einen Antrag auf Zulassung beim zuständigen Minister einzureichen. Damit ist eine rechtliche Gleichstellung der inländischen Benutzer ausländischer Datenbanken mit den Betreibern inländischer Datensammlungen gegeben. Der Antrag auf Genehmigung der Benutzung einer ausländischen Datenbank hat die in Art. 5 Abs. 3 aufgeführten Detailangaben zu enthalten; dabei dürfte die Erfüllung dieses Erfordernisses in bestimmten Fällen Schwierigkeiten bereiten, wie z.B. die Angabe der Herkunft der Daten einer ausländischen Datenbank. Mit Erteilung der Genehmigung, die - wie bei Anträgen auf Zulassung einer inländischen Datenverarbeitung - auszusprechen ist, "wenn kein Grund zur Annahme besteht, dass die Daten missbräuchlich oder entgegen den Bestimmungen des Gesetzes verwendet werden",^{267 268} erhält der Antragsteller die Berechtigung zur Benutzung der ausländischen Datenbank. De facto kommt diese staatliche Genehmigungspraxis für den Benutzer ausländischer Dateien einer Genehmigungspflicht für den Datenimport gleich, weil mit diesem Zulassungsverfahren bei Gefährdungen geschützter Interessen die behördliche Durchgriffsmöglichkeit ebenfalls gewährleistet ist. Wie weit dieses staatliche Zulassungsverfahren eine Beschränkung der Wirtschaftsfreiheit darstellt, ist von der Genehmigungspraxis abhängig und wird anhand der praktischen Erfahrungen zu beurteilen sein.

Ist einem Bewerber die Genehmigung erteilt worden, sind weitere Vorschriften zu beachten, die sich an den Benutzer der ausländischen Datenbank richten: so hat nach Art. 20 jede Person das Recht, vom Benutzer schriftlich Auskunft zu verlangen, ob die von ihm benutzte(n) Datenbank(en) ihn betreffende personenbezogene Angaben enthält und, gegebenenfalls, über deren Inhalt eine Mitteilung zu erhalten.

267 STADLER, OeVD 10/79, S. 8.

268 Aus dem Prinzip der Gleichbehandlung folgt, dass dieses Kriterium sowohl für die Beurteilung eines Antrages zur Errichtung nationaler Datenverarbeitungssysteme als auch zur Benutzung ausländischer Datensammlungen gültig ist.

Diese Regelung ist wiederum ein Ausdruck der rechtlichen Gleichstellung des inländischen Benützers ausländischer Datenbanken und Betreiber inländischer Datenverarbeitungsanlagen. Die Lösung, sich für die Geltendmachung von Ansprüchen an den 'einheimischen' Benutzer der ausländischen Datenbank halten zu können, ist sinnvoll, da durch den Zugriff auf Daten über eventuell in Luxemburg befindliche Datensubjekte die Inlandsbeziehung und besondere Bedeutung dieser Angaben im luxemburgischen Konnex evident wird.

Ausserdem kann der Träger eines Auskunfts- bzw. Einsichtsrechts nach Art. 22 i.V. mit Art. 20 fordern, dass ihn betreffende Daten berichtigt, ergänzt, klargestellt, nachgeführt oder gelöscht werden, falls sie unrichtig, unvollständig, zweideutig oder nicht mehr aktuell sind oder wenn deren Sammlung, Erfassung, Speicherung oder Uebermittlung verboten ist. Der aus dieser Bestimmung fliessende Anspruch kann sich auch an den inländischen Benutzer einer ausländischen Datenbank richten. Die Erfüllung des Anspruches durch den Benutzer kann aber u.U. problematisch sein, so z.B.:

- Die Beurteilung der Zulässigkeit der Sammlung, Erfassung, Uebermittlung oder Speicherung dieser Daten richtet sich nicht nach luxemburgischen Recht, sondern nach dem geltenden Recht desjenigen Landes, in dem die Datenbank aufgebaut ist. Eine Speicherung sensibler Daten ist z.B. nach dem BDSG nicht untersagt, so dass ein luxemburgisches Datensubjekt vom Benutzer, der eine in Deutschland befindliche Datenbank abfragt, nicht die Vornahme der Löschung der ihn betreffenden sensiblen Angaben verlangen kann, da dem luxemburgischen Gesetz im Ausland die Durchsetzungsgewalt fehlt. (U.U. kann bei der Erteilung der Genehmigung dem luxemburgischen Benutzer jedoch die Pflicht auferlegt werden, vom ausländischen Betreiber der Datensammlung eine Bestätigung beizubringen, dass dem luxemburgischen Benutzer der Zugriff auf die sensitive Daten enthaltenen Felder gesperrt wurde.)
- Die Erfüllung des Anspruches, unrichtige, unvollkommene, nicht mehr aktuelle Informationen zu berichtigen, zu ergänzen, nachzuführen oder zu löschen, kann dem Benutzer der ausländischen Datenbank

möglich aber auch unmöglich sein. Die Möglich- bzw. Unmöglichkeit ist vom systemtechnischen Benutzerprofil abhängig:

- Besitzt der Benutzer die Verfügungsgewalt über die Angaben, ist er befugt, mittels seines Terminals ändernd in den Datenbestand einzugreifen. Diesfalls kann er die Berichtigung, Nachführung, Ergänzung oder Löschung der beanstandeten Daten vornehmen und den Anspruch des Betroffenen erfüllen.
- Hat der Benutzer hingegen nur ein Einsichts- und Benutzungsrecht, aber keine Verfügungsgewalt über die gespeicherten Informationen, kann er sich die Daten zwar am Terminal ausgeben lassen, hat aber keine Möglichkeit, einen Fehler im Datenbestand selber zu korrigieren. In diesem Fall muss der luxemburgische Benutzer dem Betreiber der Datenbank im Ausland die zu ergänzen, löschen oder zu berichtigenden Daten mitteilen, damit dieser die Aenderung im Datenbestand vornehmen kann. Allerdings fehlen dem Benutzer die rechtlichen Mittel, den Vollzug der Aenderung durchzusetzen, wenn die Datenverarbeitungsanlage in einem Land ohne DSG (z.B. Belgien) lokalisiert ist. In einem Land mit DSG besteht die Wahrscheinlichkeit, dass die Angaben aufgrund des in den meisten Gesetzen verwirklichten Grundsatzes der Aktualität und Richtigkeit²⁶⁹ von Daten nachgeführt werden. Aufgabe einer internationalen Konvention könnte es sein, die Erfüllung eines solchen Individualrechtes über den territorialen Anwendungsbereich nationaler Datenschutzgesetze hinweg sicherzustellen.

c) Folgerung

Leider ist dem luxemburgischen Gesetz, das im Vergleich mit andern Datenschutzgesetzen einen restriktiven und strengen Charakter aufweist, keine ausführliche Regelung zur Ausfuhr von personenbezogenen Informationen zu entnehmen, so dass die anwendbaren Vorschriften

269 Vgl. auch Resolution (73) 22 des Europarates, 1. und 7. Grundsatz.

vom Ausland aus nur beschränkt beurteilt werden können. Die allein auf dem Anwendungsbereich fussende Vorschrift hat den Nachteil der Ausweitung des gesetzlichen Geltungsbereiches und vermag nicht alle Fragen zu beantworten.

Als positiv hingegen sind die Bestimmungen zur Dateneinfuhr zu werten, die das Bestreben zu einer klaren, am Grundsatz der Gleichbehandlung²⁷⁰ orientierten Regelung aufweisen. Singulär unter den besprochenen Gesetzen ist die explizite Feststellung des Rechts auf Auskunft auch gegenüber einem Benutzer einer im Ausland stationierten Datenbank.

Die fehlenden Begriffsdefinitionen und -umschreibungen im Gesetz, sowohl beim Export wie beim Import von Daten, erzeugen das beim institutionellen Modell charakteristische Vakuum, welches in der Regel erst durch den Erlass von Verordnungen bzw. die mit einer Genehmigung vorhandenen Bedingungen und Auflagen ausgefüllt wird.

270 Die Gleichbehandlung wird auch daraus ersichtlich, dass kein spezifischer Teil für den grenzüberschreitenden Datenverkehr im Gesetz geschaffen wurde, sondern die entsprechenden Bestimmungen zerstreut innerhalb der für das Inland geltenden Regelung vorkommen und immer auf den Fall des Importes verweisen.

III. Typenbeschreibung der rechtlichen Regelungen des grenzüberschreitenden Datenverkehrs

In den nachfolgenden Ausführungen wird das Schwergewicht auf den Export gelegt, weil dabei Daten die Rechtshoheit eines Landes verlassen und zu befürchten ist, dass die sich in einem andern Rechtskreis befindlichen, exportierten Daten - in Ermangelung des Schutzes der im Herkunftsland bestehenden Gesetze - weniger oder überhaupt nicht geschützt sind und die Gefahr eines Missbrauches ansteigt. Jeder Gesetzgeber ist daher geneigt, dem Export von Daten bei der rechtlichen Ausgestaltung des grenzüberschreitenden Datenverkehrs mehr Gewicht zu verleihen, indem er den im Inland geltenden Schutz auszudehnen versucht. Dies wird häufig in der Form verwirklicht, dass er den Export von bestimmten Voraussetzungen abhängig macht, die Gewähr bieten sollen, dass der Schutz der Daten auch im Ausland sichergestellt ist.

Die Bestimmungen über den Import sind dabei aber nicht weniger wichtig: die qualifizierte Regelung des Datenexportes lässt sich entsprechend auf eine Regelung der Importe anwenden, da der Gesetzgeber "weder die unkontrollierte Uebermittlung personenbezogener Angaben ins Ausland hinnehmen, noch sich mit einer uneingeschränkten Einfuhr derartiger Daten abfinden" ²⁷¹ kann. Praktisch wird sich das nachfolgend ²⁷² für den Export dargestellte Genehmigungssystem nicht in allen seinen Ausprägungen auf den Import anwenden lassen, sondern sich nur in bestimmten Formen (z.B. beschränkt freier Import mit Verbotsvorbehalt) als geeignete Lösung der Einfuhr von Daten erweisen. Die Bedeutung des Lizenzierungs- bzw. Genehmigungssystems liegt in der Sicherstellung einer Möglichkeit zur wirksamen Ueberwachung der eingeführten Daten, die eine behördliche Durchgriffsmöglichkeit gewährleistet, falls die aus dem Ausland importierten Informationen Persönlichkeitsrechte von im Inland befindlichen Personen zu beeinträchtigen vermögen. Die Regelung über den Datenimport hat einen

271 SIMITIS, Festschrift, S. 368.

272 Vgl. hinten, S. 224.

eigenen Stellenwert²⁷³ im Bereich des grenzüberschreitenden Datenverkehrs; ihre vermeintlich sekundäre Bedeutung ergibt sich aus der Tatsache der in den europäischen Datenschutzgesetzen vorgenommenen Gleichstellung und Gleichbehandlung²⁷⁴ von personenbezogenen Daten inländischer und ausländischer Provenienz; m.a.W., solange die Datenverarbeitung im Inland erfolgt, ist für den Schutz der Daten unerheblich, ob sie Inländer oder Ausländer betreffen, ob die Daten aus dem Inland oder Ausland stammen, noch, wer ihre Verarbeitung durchführt - entscheidend ist alleine die Durchführung der Verarbeitungsaktivitäten im Inland. Aus dem Ausland stammende Angaben treten dadurch automatisch unter den Geltungs- und Anwendungsbereich des Gesetzes des Importlandes, d.h. das dem Gesetzgeber vertraute, von ihm selbst erlassene Schutzsystem (von dessen Wirkungskraft er aus subjektiven Gründen überzeugt ist), ist auf die eingeführten Daten anwendbar. Die spezifische Bedeutung einer Regelung des Datenimportes ist m.E. darin zu sehen, dass der Gesetzgeber die Absicht manifestiert, "seine Massstäbe auf jede das Inland berührende Datenverarbeitung anzuwenden."²⁷⁵ Ohne Bekundung dieser Absicht (die ausdrückliche Unterstellung der eingeführten Informationen unter das inländische Gesetz) ist der Schutz zumindest aller im Inland befindlichen Personen nicht zu verwirklichen. Die importierten Daten sollten den gleichen Zulässigkeitsvoraussetzungen zur Bearbeitung unterstellt werden wie die inländischen Daten; ein behördliches Durchgriffsrecht zur Aktualisierung dieses Schutzes beim Import sollte m.E. nur als Notbremse (ultima ratio) wirken.

Zwischen den beiden Extremen einer Regelung des grenzüberschreitenden Datenverkehrs, d.h. zwischen einem Exportverbot für personenbezogene Daten und einem freien, uneingeschränkten Export von Informationen existieren die verschiedensten Abstufungen, die sich in national unterschiedlichen Ausprägungen manifestieren. Beim Versuch, diese

273 Gl.M. SIMITIS, a.a.O., S. 363.

274 Im Gegensatz zum Privacy Act von 1974 (Sect. 552 [a] 2), der den Schutz beschränkt auf "a citizen of the United States or an alien lawfully admitted for permanent residence".

275 SIMITIS, a.a.O.

zu klassieren und zu typisieren, ergeben sich zwei verschiedene Grundformen einer rechtlichen Regelung:

- Die eine Gruppe umfasst die Regelungen mit einem System von behördlichen Eingriffsmöglichkeiten und erfährt deshalb ihre rechtliche Ausgestaltung durch die Abstufungen²⁷⁶ der Genehmigungsverfahren; entscheidend für diese Gruppe ist die öffentlichrechtliche Durchgriffsgewalt, welche lenkend bzw. schützend auch auf internationaler Ebene eingreifen kann.
- Die andere Gruppe rechtlicher Ausgestaltung kennt keine behördliche Eingriffsmöglichkeit, weder als Generalklausel noch als spezielles Genehmigungssystem und wird deshalb als sog. genehmigungsfreier Datenexport bezeichnet.²⁷⁷

1. Absolutes Exportverbot

Das eine Extrem besteht in einer rechtlichen Regelung, die jeden Export manuell oder automatisiert zu verarbeitender personenbezogener Informationen sowohl für öffentliche als auch private Rechtsträger von Datensammlungen absolut, d.h. gegenüber allen ausländischen Staaten verbietet. Diese Erscheinungsform ist bisher in keinem der erlassenen Datenschutzgesetze oder diskutierten Entwürfen aufgetaucht, weil sie wirtschaftlich nicht vertretbar,²⁷⁸ informationell systemwidrig,²⁷⁹ politisch nicht haltbar²⁸⁰ und rechtlich nicht durchsetzbar²⁸¹ ist, da der Kommunikation als solcher, insbesondere

276 Einzelgenehmigung, Mustergenehmigung, Konzession, beschränkt freier Export mit Verbotsvorbehalt, vgl. hinten, S. 224ff.

277 Vgl. hinten, S. 223ff.

278 Vgl. vorne, S. 11.

279 Die heutigen Technologien der Informatik sind auf Kommunikation ausgerichtet mit denen geographische oder nationale Grenzen mühe-los überbrückt werden können.

280 Vgl. vorne, S. 8, 11, 44f. und 223; ferner aber auch bezüglich Ländern, die politisch sich zu den gleichen Grundwerten bekennen, z.B. westliche Industriestaaten, OECD-Staaten etc., u.U. aber auch gegenüber Entwicklungsländern und Comecon-Staaten.

281 Es wäre z.B. auch nicht möglich, den Export sachbezogener Daten zuzulassen, die Ausfuhr personenbezogener Information dagegen generell zu verbieten.

aber auch dem internationalen Datenaustausch (z.B. im Rahmen der internationalen Handelsbeziehungen) immer mehr Bedeutung zukommt.²⁸² Mit einem absoluten Exportverbot ist zwar der Gesetzgeber der Kontrolle der im Inland in Datensammlungen gespeicherten und zum Export bestimmten Angaben enthoben, er vermag aber den Bürgern keinen vollkommenen Schutz vor Speicherung ihrer Daten im Ausland zu gewähren: aus der Mobilität der Gesellschaft folgt, dass ein Individuum bei seinen Aufenthalten im Ausland "Datenspuren"²⁸³ hinterlässt, die im Falle eines Exportverbotes, mangels Verfügbarkeit bzw. Export zusätzlicher relevanter Daten von den speichernden Stellen des Ursprungslandes, notwendigerweise lückenhaft sein würden. Damit würde - überspitzt ausgedrückt - die Gefahr heraufbeschworen, dass Stellen im Ausland versuchen könnten, mit den vorhandenen Daten ein Persönlichkeitsbild aufzubauen, das aufgrund der fragmentarisch und begrenzt verfügbaren Merkmalen nur unvollkommen sein kann. Durch eine solch lückenhafte Speicherung in ausländischen Datensammlungen entsteht für den Betroffenen überdies die Gefahr der Diskretisierung. Durch das Verbot des Exportes hindert der Gesetzgeber die personenbezogene Angaben benötigenden Stellen im Ausland, sich über das Datensubjekt ein informationell "abgerundetes",²⁸⁴ d.h. möglichst vollständiges, richtiges und aktuelles Persönlichkeitsbild über den Betroffenen zu schaffen.

Werden von einem Gesetz nur die automatisiert verarbeiteten Daten geschützt und von einem Exportverbot betroffen, könnte eine Umlagerung der Verarbeitung auf manuelle Verfahren für diejenigen Daten erfolgen, die im Ausland benötigt werden, d.h. auf dem Umweg der manuellen Bearbeitung wird die Möglichkeit zur Ausfuhr von Daten gesucht.

In bestimmten Fällen kann ein Exportverbot gegenüber gewissen Staaten angebracht sein, z.B. bei data havens, um den Export und einen dadurch möglichen Missbrauch von Daten zu unterbinden. M.E. ist

282 Vgl. § 1, vorne, S. 8.

283 Z.B. Personalangaben bei Einreisen, bei Hotelübernachtungen, Daten von Checkabrechnungen, Kreditkarten etc.

284 Soweit ein durch Einzelangaben aufgebautes Persönlichkeitsbild vollständig und abgerundet sein kann, was m.E. zu bezweifeln ist.

aber eine solche informatorische Isolation gegenüber Drittstaaten nur als ultima ratio einzusetzen. Dabei ist zu bedenken, dass ein derartiger "Datenvorhang" nur dann wirksam ist, wenn einerseits mehrere Staaten (z.B. alle Mitgliedstaaten einer Konvention) daran beteiligt sind und andererseits sowohl die manuell als auch automationsunterstützt verarbeiteten Informationen dem Ausfuhrverbot unterstehen.

2. Exportverbot mit Erlaubnisvorbehalt

A. Begriff

Das Exportverbot mit Erlaubnisvorbehalt bedeutet nach dem Extrem des absoluten Verbotes eine Lockerung in dem Sinne, dass unter bestimmten Voraussetzungen oder für gewisse Fälle eine behördliche Erlaubnis zum Export von Daten erteilt werden kann. Der Grundgedanke dieses Systems besteht darin, den Datenexport zwar grundsätzlich zu verbieten, das Prinzip aber für bestimmte Fälle mit einer Erlaubniserteilung zu durchbrechen. Damit ist die Kontrolle, d.h. der behördliche Durchgriff sichergestellt, dessen harte und unmittelbare Wirkung wird aber durch die Möglichkeit der Erteilung einer Ausfuhrbewilligung abgeschwächt und macht das Prinzip nicht starr.

Eine rechtlich unterschiedliche Ausprägung erhält das hier nur noch dem Grundsatz nach existierende Exportverbot durch eine differenzierte Ausgestaltung des Erlaubnisvorbehaltes mittels Abstufungen innerhalb des Genehmigungssystems.

B. Abstufungen des Genehmigungssystems

a) Einzelgenehmigung

Das Instrument der Einzelgenehmigung bildet die erste Stufe unter den möglichen des Genehmigungssystems und schafft eine materiell restriktive Ausgestaltung des Erlaubnisvorbehaltes. Das Prinzip der Einzelgenehmigung hat zur Folge, dass für jeden Fall eines Exportes von Daten ins Ausland eine Genehmigung bei der zuständigen Behörde einzuholen ist. Das Behördenorgan überprüft anhand der individuellen und konkreten Situation²⁸⁵ die Erteilung oder Verweigerung der Exportgenehmigung.²⁸⁶

Mit dem System der Einzelgenehmigung kann die Datenausfuhr genau kontrolliert und, falls notwendig, unterbunden werden; dieses Verfahren erweist sich auch als geeignetes Mittel, protektionistische Ziele zu verfolgen. Nachteile kann der als Einzelgenehmigung ausgestaltete Erlaubnisvorbehalt nicht nur den datenverarbeitenden Rechtsträgern, sondern auch den mit der Kontrolle beauftragten Behörden und in bestimmter Hinsicht der gesamten Gesellschaft bringen:

- Für den Datenverarbeiter bedeutet das Einholen von Einzelgenehmigungen eine spürbare Belastung beim beabsichtigten Export von personenbezogenen Informationen.
- Die mit der EDV erzielten Vorteile der Beschleunigung der Verarbeitungsabläufe können durch die bis zur Erteilung einer Ausfuhrerlaubnis entstehenden Wartezeiten zunichte gemacht werden. Bei einer Anwendung dieses Prinzips müsste daher m.E. dem Antragsteller eine ihm zumutbare, kurze Zeitspanne bis zur Erteilung einer Genehmigung bzw. Abweisung garantiert werden.
- Die datenverarbeitenden Stellen,²⁸⁷ die einer solchen Regelung unterstehen, sind gegenüber Ländern, die innerhalb von Datenschutz-Staaten einen "beschränkt freien Export, bzw. Austausch"²⁸⁸ pflegen dürfen, benachteiligt.
- Für die Genehmigungsbehörden bringt eine individuelle Beurteilung jedes Exportfalles (und deren konkrete Ueberprüfung der Auswirkungen bei einem Passieren der Daten über die nationalen Grenzen) eine intensive Beanspruchung und Belastung, insbesondere wenn der Entscheid innerhalb einer gewissen Frist erfolgen muss.
- Nicht praktikabel sind Einzelgenehmigungen bei wiederholtem direkten Zugriff auf inländische Datenbanken vom Ausland her:

285 Natur, Art, Inhalt der personenbezogenen Daten; Zahl der vom Export betroffenen Datensubjekte; Empfängerland der Daten und der dort geltende Schutz durch die nationale Rechtsordnung etc.

286 Vgl. bestimmte Fälle in Schweden: vorne, S. 193f., Anm. 204.

287 D.h. Industrie, Wirtschaft etc. und öffentlicher Sektor.

Einzelgenehmigungen bedingen einen zu grossen administrativen Aufwand, als dass für jeden Zugriff eine individuelle Abklärung des konkreten Falles vertretbar wäre - das Prinzip der Verhältnismässigkeit ist gestört. Ausserdem würde damit auch die Ausnützung inländischer Computerkapazität durch ausländische Stellen negativ beeinflusst.

- Durch die restriktive Handhabung des Datenexportes findet eine gewisse Lähmung des internationalen Datenaustausches im betreffenden Lande statt, d.h. die inländischen Datenverarbeiter könnten zum Schluss kommen, von vorneherein auf ein Gesuch für die Bewilligung des Datenexportes zu verzichten, weil der Bewerber seine Chance für eine Gutheissung des Antrages als zu gering einschätzt, oder weil ihm der administrative Aufwand für das Bewilligungsverfahren zu gross erscheint. Die in Schweden festgestellten Auswirkungen des Datalagen auf den grenzüberschreitenden Datenverkehrs sind unter Berücksichtigung dieser Aspekte nur schwer zu beurteilen.²⁸⁹

In dieser reinen Form wird ein System von Einzelgenehmigungen auf den grenzüberschreitenden Datenverkehr mehrheitlich negative Folgen haben, wie sie vorgängig aufgezählt wurden.

Hingegen kann der Vorbehalt der Einzelgenehmigung für einen gezielten Einsatz innerhalb eines liberalen Exportsystems durchaus seine Berechtigung haben oder sogar erforderlich sein, um eine Differenzierung der behördlichen Durchgriffsmöglichkeit zu erreichen: so könnte sie z.B. eine wirksame und geeignete Waffe gegenüber "data havens" darstellen.

b) Mustergenehmigung

Die Erteilung einer Mustergenehmigung stellt die nächsthöhere Stufe in einem Genehmigungssystem dar. Sie ermöglicht eine wesentlich flexiblere Ausgestaltung des Erlaubnisvorbehaltes. Die Mustergenehmi-

288 Vgl. hinten, S. 231ff.

289 Vgl. auch TDR, Vol. 1, No. 3, 1978, S. 3.

gung bewirkt, dass die für die Ausfuhrbewilligung zuständige Behörde nicht eine minuziöse Ueberprüfung jedes konkreten Exportfalles vornehmen muss, sondern einem Gesuchsteller für eine bestimmte Art von Daten den Export in bestimmte Staaten bewilligen kann. Mit der Mustergenehmigung erhält der Gesuchsteller das Recht, Daten der bewilligten Art so oft wie es die Erfüllung der mit der Datenverarbeitung zu erledigenden Aufgabe erfordert an den betreffenden Empfänger oder eine Gruppe von Adressaten ins Ausland zu übermitteln.

- Der Vorteil der Mustergenehmigung liegt in der höheren Praktikabilität, im Sinne der mehrfachen Exportmöglichkeit bestimmter Datenarten an einen oder mehrere ausländische Empfänger.
- Auch hier kann eine umfassende Kontrolle der Datenausfuhr durchgeführt und gegebenenfalls ein Export verweigert werden. Hat die Ueberprüfung der konkreten Sachlage jedoch ergeben, dass mit einer Ausfuhr keine schutzwürdigen Belange von Datensubjekten betroffen werden, kommt der Genehmigung eine weitergehende Bedeutung zu: Der Export wird für eine konkrete Situation bis zum Eintritt einer Aenderung generell zugelassen.
- Die Tätigkeit der Behörde beschränkt sich bei der Mustergenehmigung auf eine einmalige Prüfung des Sachverhaltes bei der Antragstellung, so dass eine mehrfache Belastung der Behörden durch ein iteratives Bewilligungsverfahren wie im Falle der Einzelgenehmigung entfällt.
- Durchführbar ist das System der Mustergenehmigungen auch für den Zugriff auf inländische Datenbanken durch Stellen im Ausland. Weil i.d.R. ein direkter Zugriff wiederholt auf die gleiche Datenbank erfolgt und dabei identische Datenarten abgefragt bzw. ausgeführt werden, erweist sich - bei einer Befürwortung der grundsätzlichen Durchgriffsmöglichkeit - das Prinzip der Mustergenehmigung als geradezu ideal.

Dies bewirkt indirekt eine Oeffnung des inländischen Verarbeitungsangebotes für Stellen im Ausland und damit eine mögliche Förderung der Nutzung inländischer Computerkapazität durch ausländische Datenverarbeiter.

- Durch die repetitive Exportmöglichkeit an einen bestimmten Adressaten oder eine Gruppe von Empfängern ist die Benachteiligung inländischer Verarbeiter gegenüber ihren Mitbewerbern in einem Staat, welcher den freien oder 'beschränkt freien' Verkehr zulässt, nicht mehr so schwerwiegend wie bei der Einzelgenehmigung.
- Nachteilig kann sich die Mustergenehmigung u.U. auswirken, wenn sie generell die Einzelgenehmigung ausschliesst, so dass keine Ueberprüfung einzelner besonders heikler Datenexporte mehr stattfindet.

Die Mustergenehmigung kann insgesamt als liberale Ausgestaltung des auf dem Exportverbot beruhenden Erlaubnisvorbehaltes gewürdigt werden, die einen ausgewogenen Ausgleich zwischen gegensätzlichen Interessen, dem Bestreben auf Gewährleistung von Kontrolle und besonderem Schutz internationaler Datenflüsse und dem Interesse an minimalen behördlichen Eingriffen herstellen kann. Der Umstand, dass verschiedene Datenschutzgesetze diese Lösung gewählt haben²⁹⁰ unterstreicht ihren Stellenwert in der Datenschutzgesetzgebung, sei es als komplementäres Instrument zu andern Genehmigungstypen, sei es als vorherrschende Regelungsart.

c) Konzession

Die Konzession stellt eine weitere Stufe innerhalb des Genehmigungssystems dar, in dem der Erlaubnisvorbehalt eine noch liberalere Ausgestaltung erfährt, die behördliche Durchgriffsmöglichkeit aber immer noch gewahrt bleibt.

Die Konzession ist gegenüber der Mustergenehmigung inhaltlich umfassender, indem sie dem Inhaber bzw. der datenverarbeitenden Stelle eine generelle Erlaubnis zum wiederholten Export von Daten verschiedenster Art und Natur an einen bestimmten Adressatenkreis (z.B. Mutter- und Tochtergesellschaften oder zu einem Konzern gehörende

290 Z.B. Oesterreich, Dänemark.

nationale Gesellschaften und Niederlassungen) in einer nicht festgelegten Anzahl von Ländern erteilt. Die Konzession geht insofern weiter, als der Inhaber zur Datenausfuhr an einen grösseren Adressatenkreis befugt ist, diese Datenempfänger zudem nicht in einem bestimmten, sondern in verschiedenen Ländern ansässig sein können und schliesslich nicht nur eine bestimmte Art, sondern mehrere Datenarten personenbezogener Natur übermittelt werden können, soweit dies für die Erfüllung des konzessionierten Geschäftszweckes notwendig ist. Die Erteilung einer Konzession fusst auf einer 'einmaligen' Beurteilung und Analyse ²⁹¹ des Antragstellers und seines beabsichtigten Exportvorhabens; diese Ueberprüfung wird erhöhte Sorgfalt erfordern, um eine solche Konzession nicht ihrer Wirkungskraft zu berauben und dem Inhaber einen Freipass zum Export von Daten zu geben. Eine periodische behördliche Kontrolle der Voraussetzungen, die zur Erteilung der Genehmigung geführt haben, wird zusätzlich notwendig sein und den Inhaber zur Beachtung aller internen Verhaltensrichtlinien und Massnahmen, die den Schutz der Persönlichkeit sicherstellen, anhalten. ²⁹²

Diese umfassende Ermächtigung zum Datenexport - evtl. auch an Adressaten in Ländern, die noch kein Datenschutzrecht haben - spiegelt das Vertrauen der Genehmigungsbehörde in die Loyalität und datenschutzgerechte Handlungsweise des Konzessionsinhabers. Voraussetzung ist allerdings, dass beim Konzessionär betriebsinterne Massnahmen getroffen werden, die einen hohen Schutzstandard und ein ausgereiftes Datensicherungssystem gewährleisten. Bekanntestes Beispiel dafür ist

291 Aufbau der Datenbanken, Art und Natur der Daten, Organisationsstruktur der Datenverarbeitung, Datensicherung, evtl. Aufbau der Datennetze und damit zusammenhängende Schutz- und Sicherungsvorkehrungen, etc.

292 Die Möglichkeit des Entzuges einer Konzession bei (grober) Zuwiderhandlung oder schwerwiegender Persönlichkeitsverletzung wird dabei auch eine gewisse repressive Wirkung zur Einhaltung und Beachtung der Schutzvorschriften ausüben.

die Konzessionserteilung an die SWIFT-Mitgliederbanken in Schweden.^{293 294}

Mit der Erteilung einer Konzession wird ein multinational operierendes Unternehmen nicht etwa für alle seine Informationsflüsse dem nationalen Recht unterstellt, sondern nur einem dem inländischen Recht unterworfenen Bearbeiter die Befugnis erteilt, in dem in der Konzession festgelegten Umfang den Datenaustausch mit seinen ausländischen Geschäftspartnern bzw. zum Konzernverbund gehörenden Gesellschaften zu pflegen. (Es ist auch denkbar, dass der nationale Rechts-träger die Verpflichtung auf sich nehmen muss, dafür zu sorgen, dass die an einen ausländischen Dritten weitergeleiteten Daten, wenn sie an weitere Empfänger gelangen, auch bei jenen entsprechend zu schützen sind.)

Der Fall Schweden beweist, dass eine Konzession durchaus neben dem Institut der Einzel- oder Mustergenehmigung ihren Stellenwert hat; sie hat sogar im Rahmen eines beschränkt freien Exportes²⁹⁵ ihre Berechtigung, vor allem für die Fälle, in denen ein Konzern eine weitere geographische Verbreitung aufweist, als sie durch einen beschränkt freien Export abgedeckt werden könnte. Diese Form der Export-erlaubnis kommt der Forderung des freien Datenaustausches weit entgegen, weist aber durch das Erfordernis der Konzessionserteilung eine subjektive Ausprägung auf. In der heute geltenden Konstellation von Rechtsordnungen mit national unterschiedlicher Ausgestaltung des Datenschutzes ohne verbindendes internationales Abkommen stellt das Instrument der Konzession eine mögliche Form dar, für die exportierten Daten einen angemessenen Schutzstandard zu gewährleisten.

293 Vgl. vorne, S. 193f., Anm. 38.

294 Vgl. vorne, S. 67ff.

295 Vgl. nachfolgend Nr. 3., S. 231.

3. 'Beschränkt freier' Datenexport mit Verbotsvorbehalt

A. Systematische Einordnung

Diese Ausprägung einer rechtlichen Regelung des grenzüberschreitenden Datenverkehrs steht im Schnittpunkt der beiden Grundtypen, so dass ihre Ausgestaltung über beide Lösungsansätze erreicht werden kann:

a) Einreihung unter das Exportverbot mit Erlaubnisvorbehalt

Diese Erscheinungsform stellt die letzte Stufe des Exportverbotes mit Erlaubnisvorbehalt dar: die rechtliche Konstruktion erfolgt in dem Sinne, dass der Erlaubnisvorbehalt seine Ausgestaltung für bestimmte Tatbestände nicht durch eine besondere Form der Genehmigung erhält, sondern durch den Verzicht auf das Erfordernis der Genehmigung schlechthin. So wird in Ausnahmefällen, unter einem dem Grundsatz nach weiterhin existierenden Exportverbot, der Inhalt des Erlaubnisvorbehaltes ein Verzicht auf eine die Erlaubnis gestaltende Form darstellen.

b) Einreihung unter den genehmigungsfreien Datenexport

Die Einstufung unter den genehmigungsfreien Datenexport ²⁹⁶ ist hier offensichtlich und braucht nicht ausführlich erläutert zu werden. Der Datenexport ist grundsätzlich frei, unter Vorbehalt der Erfüllung der gesetzlichen Voraussetzungen. Als charakterisierendes Element dieser Bedingungen tritt ein Bestandteil des andern Grundtypus hinzu, d.h. ein behördliches Durchgriffsrecht als ultima ratio in Form eines Verbotsvorbehaltes, woraus sich eine Mischung von Elementen beider Typen ergibt.

c) rechtlicher Unterschied und Konsequenz

Die Einreihung unter das grundsätzliche Exportverbot erlaubt der Behörde, den in einem Verzicht auf eine bestimmte Genehmigungsform bestehenden Erlaubnisvorbehalt an das Vorhandensein bestimmter Gege-

296 Vgl. vorne, S. 222 und nachfolgend Nr. 4), S. 234ff.

benheiten und Voraussetzungen zu knüpfen, womit bei deren Nichterfüllung oder Fehlen der Inhalt dieses Erlaubnisvorbehaltes gegenstandslos wird und sich automatisch die entsprechende behördliche Durchgriffsmöglichkeit ergibt. Die Abhängigkeit des genehmigungsfreien Datenexportes von diesen Voraussetzungen bildet die Grundlage für den Begriff 'beschränkt freier' Datenexport.

Aus der Einstufung des beschränkt freien Datenexportes unter den Grundtypus der genehmigungsfreien Ausfuhr ergibt sich die Abhängigkeit des Exportes von bestimmten Voraussetzungen. Falls diese Grundbedingungen nicht mehr erfüllt sind, hat die zuständige Behörde die Befugnis, den beschränkt freien Datentransfer mit dem Instrument des Verbotsvorbehaltes zu unterbinden. Materiell muss dieser Verbotsvorbehalt auf einer gesetzlichen Grundlage beruhen, so dass die den Export untersagende Behörde sich darauf abstützen und der Bearbeiter sein Verhalten danach ausrichten kann, da sie die Beweislast für den Eingriff und die Beschränkung der gesetzlich eingeräumten Ausfuhrfreiheit erbringen muss.

B. Inhalt des beschränkt freien Exportes

Die beschränkt freie Datenausfuhr stellt gegenüber der Konzession eine noch weitergehende Liberalisierung dar und gibt den datenverarbeitenden Rechtsträgern eines Landes die Befugnis, ohne irgendeine Genehmigung Informationen, die alle²⁹⁷ oder nur bestimmte²⁹⁸ Rechtssubjekte betreffen, an Empfänger in gewissen ausländischen Staaten zu übermitteln. Normadressaten sind alle im Inland befindlichen Stellen, die personenbezogene Daten verarbeiten. Der "freie" Export ist dabei relativiert zu verstehen i.S. von genehmigungsfrei und soweit er zu Erfüllung eines legitimen Geschäftszweckes notwendig ist. Charakteristisch ist die Beschränkung der genehmigungsfreien Ausfuhr auf Destinationsländer mit einer ausreichenden Daten-

297 D.h. natürliche und juristische Personen (u.U. inklusive Personengruppen).

298 Z.B. nur natürliche Personen.

exportregelung. Diese Beschränkung resultiert aus der Erfüllung der für den genehmigungsfreien Export geforderten Voraussetzungen.

C. Voraussetzungen

Die Voraussetzungen werden in den einzelnen Gesetzen umschrieben und sind weitgehend in der immer wieder auftauchenden Grundformel beinhaltet: Der (genehmigungsfreie) grenzüberschreitende Datenverkehr ist dann erlaubt, wenn sichergestellt ist, oder zumindest eine genügende Gewissheit besteht, dass für den Umgang und die Verarbeitung mit den weitergegebenen Daten im Ausland Grundsätze und Bestimmungen vorhanden sind, die den für das Inland aufgestellten Prinzipien entsprechen und den Datensubjekten einen vergleichbaren Schutz gewähren, so dass Grund zur Annahme besteht, dass die Weitergabe der personenbezogenen Angaben zu keiner unzulässigen Gefährdung der Betroffenen führen wird.²⁹⁹ Diese Formel reflektiert die Bemühungen des Gesetzgebers, den exportierten Daten bzw. den Datensubjekten einen möglichst gleichen Schutz wie im Inland zukommen zu lassen. Bei Erfüllung dieser Voraussetzungen ist er gewillt, das behördliche Durchgriffsrecht (z.B.) ganz in den Hintergrund zu stellen und die Datenausfuhr ohne Genehmigung zu gestatten.

D. Bedeutung

Dem beschränkt freien Datenexport kommt m.E. eine zentrale Bedeutung zu, vor allem zwischen Staaten, die ebenfalls Datenschutzgesetze erlassen haben oder zwischen Staaten einer zukünftigen Konvention, um innerhalb dieses geschützten, geschlossenen Raumes den freien Datenfluss zu verwirklichen. Diese Exportart ist die geeignete Form, die

299 Diese Norm ist in einigen Datenschutzgesetzen enthalten, z.B. BDSG (§ 24, vgl. vorne, S. 147f.), DSG (§ 32 Abs. 2 Ziff. 2, vgl. vorne, S. 177), Datalagen (§ 11, vgl. vorne, S. 193) etc.

divergierenden Forderungen³⁰⁰ auf einen Schutz personenbezogener Daten einerseits und auf Gewährleistung des freien Datenflusses andererseits, wenn auch für letzteres nur in beschränktem³⁰¹ Umfange, zu verwirklichen. Bei dieser Regulationsart wird die unterschiedliche Behandlung der Staaten mit Datenschutzgesetzen und Ländern ohne Datenschutzbestimmungen ersichtlich. Diese Differenzierung hat ihren Ursprung in der fehlenden Bereitschaft gewisser Länder, Datenschutzregelungen zu erlassen, so dass die Datenschutzstaaten veranlasst werden, den internationalen Datenverkehr mit diesen Nationen "durch Dirigismen zu beschränken und damit die internationalen Handelsbeziehungen Objekt einer Fremdkontrolle werden zu lassen",³⁰² um eine Entstehung von "data havens"^{303 304} zu verhindern; hingegen wird mit der Zulassung eines beschränkt freien Datenverkehrs der ökonomischen Notwendigkeit des freien Informationsflusses unter Datenschutzstaaten Rücksicht getragen und einem möglichen informationellen Protektionismus entgegengesteuert.

4. Genehmigungsfreier Datenexport

A. Begriff

Diese Kategorie der rechtlichen Ausgestaltung stellt das Gegenstück zum Genehmigungssystem dar und charakterisiert sich durch das Fehlen eines behördlichen Durchgriffsvorbehaltes in Form einer Genehmigung oder andern Generalklausel. Der Gesetzgeber hat weder ein grundsätzliches Exportverbot noch einen Genehmigungs- bzw. Verbotsvorbehalt erlassen und sich auch kein anderes (rechtliches) Mittel vorbehalten, um im Spezialfall des grenzüberschreitenden Datenverkehrs bei einer Gefährdung der ratio legis einen behördlichen Durchgriff vornehmen zu können. Unter genehmigungsfreiem Export ist das Nichtvorhandensein einer Bestimmung oder Generalklausel zu verstehen, die

300 Vgl. vorne, S. 23ff.

301 Beschränkt auf Datenschutz-Staaten bzw. Konventionsländer.
302 KASPERS, DS+DS 2/80, S. 84.

303 D.h. eine Umgehung des eigenen Gesetzes.

304 Vgl. vorne, S. 33ff.

einer Behörde die Möglichkeit verschaffen würde, in ausserordentlichen Fällen bei der Weitergabe von Daten sowie dem grenzüberschreitenden Dateiverkehr einen korrigierenden Eingriff zu vollziehen.

B. Erscheinungsform

Mit dem Fehlen eines solchen Instituts (Genehmigung, Durchgriffsrecht schlechthin) ist allerdings noch keineswegs gesagt, dass der Export von Daten absolut frei ist: er kann vielmehr mittels abgestufter gesetzlicher Anforderungen oder Voraussetzungen in verschiedenen Nuancierungen beschränkt werden, wobei das gleiche Spektrum der rechtlichen Ausgestaltung erfasst ist, - von restriktiven Vorschriften bis zum beschränkt freien Export - wie es innerhalb des Genehmigungssystems vorkommt. Die Voraussetzungen für einen Export können sogar derart hochgeschraubt werden, dass sie nicht mehr erfüllbar sind und damit de facto einem Exportverbot gleichkommen, ohne dass ein solches speziell erlassen werden müsste. Die Anforderungen können aber auch so niedrig angesetzt werden, dass sie einem freien Datenexport gleichkommen. Die absolut freie Datenausfuhr stellt die letzte Verwirklichungsstufe des genehmigungsfreien Systems dar.

Die Grundlage des absolut freien Datenexportes kann nun einerseits in der Existenz eines Gesetzes, andererseits aber auch in dessen Nichtexistenz gegeben sein: im ersten Fall garantiert ein Gesetz den freien Datenexport und schliesst dabei jede behördliche Eingriffsmöglichkeit a priori aus, oder die absolut freie Datenausfuhr ist (wie im zweiten Fall) die Folge der Nichtexistenz jeglicher Vorschriften und Eingriffsmöglichkeiten, so dass in der entsprechenden Rechtsordnung hinsichtlich des grenzüberschreitenden Datenverkehrs keine einschränkenden Vorschriften existieren und er demnach, mangels Vorschrift, absolut frei ausgeführt werden kann.

Die mit einem absolut freien Datenexport verbundene Problematik ist weitgehend bekannt und bereits dargestellt worden.³⁰⁵ Hinzuweisen ist an dieser Stelle nochmals auf die Gefahr der Isolierung durch Datenschutzstaaten aus dem Erlass einer restriktiven Ausfuhrregelung und dem damit entstehenden Datenvorhang gegenüber "data havens".

C. Folgerung

Das genehmigungsfreie System hat vor allem im Bereich der restriktiveren Ausgestaltungsformen³⁰⁶ den Nachteil, dass es starr, unbeweglich und schwerfällig ist. Wenn damit eine differenzierte Regelung realisiert werden soll, unter Ausschöpfung des gesamten Spektrums der möglichen Erscheinungsformen internationaler Datenflüsse, ist eine Vielzahl verschiedener Bestimmungen notwendig, die in einer enumerativen Aufzählung der möglichen Fallvarianten enden können; dies erscheint als notwendige Konsequenz eines Verzichtes auf behördliche Eingriffe bei der Verwirklichung des Persönlichkeitsschutzes im grenzüberschreitenden Datenverkehr. Eine Mehrzahl von Regelungstatbeständen kann zudem auf die Bearbeiter abschreckend und hemmend wirken, so dass m.E. dem flexibleren Genehmigungssystem der Vorzug zu geben ist. Die Starrheit des genehmigungsfreien Systems ist auch weniger geeignet, der in einer schnellen Entwicklung befindlichen Datenverarbeitungstechnologie und -methodik im 'Notfalle' adäquat entgegenzutreten.

Das Ausmass der Freiheit beim grenzüberschreitenden Datenverkehr ist letztlich nicht vom genehmigungsfreien System abhängig, sondern wird durch die rechtliche Ausgestaltung des Prinzips gekennzeichnet.

5. Schlussfolgerung

Aus der Praxis der vorhandenen gesetzlichen Lösungen ergibt sich, dass man sich zum einen oder andern Prinzip - dem Genehmigungssystem oder dem genehmigungsfreien Modell - bekennen kann. Diese verschiedenen Regelungstypen des grenzüberschreitenden Datentransfers sind nun nicht notwendigerweise mit einem der Gesetzesmodelle³⁰⁷ gekoppelt: In der Regel steht dem institutionellen Modell das Genehmigungssystem näher, da das institutionelle Organ seine Aufsichtsfunktion durch die Erteilung von Genehmigungen wahrnehmen kann; anderer-

305 Vgl. I. Teil.

306 Entsprechend den Stufen der Einzel-, bzw. Mustergenehmigung oder Konzession.

307 Vgl. vorne, S. 189ff.

seits ist das organisatorische Gesetzesmodell keineswegs mit dem genehmigungsfreien Regelungstypus verknüpft. Das Genehmigungssystem gibt durch seine Anpassungsfähigkeit an wechselnde Tatbestände dem organisatorischen Modell einen Grad von Flexibilität, der für das institutionelle Modell charakteristisch ist. Die Kombination 'organisatorisches Modell - Genehmigungssystem' ist m.E. geradezu eine optimale Zwischenstufe.

Innerhalb eines Systems ist für die Erfassung des grenzüberschreitenden Datenverkehrs nicht mit einer Regelungsstufe (z.B. Mustergenehmigung oder beschränkt freier Export) auszukommen; die verschiedenen Formen der Abstufung können und müssen nebeneinander auf die verschiedenen Ausprägungen des Datenverkehrs³⁰⁸ angewandt werden: Ein absolutes Exportverbot kann gegenüber einer bestimmten Nation seine Berechtigung haben, sei es aus Gründen der nationalen Sicherheit oder aus rechtspolitischen Ueberlegungen (Vermeidung von data havens); genauso kann eine Konzession innerhalb eines beschränkt freien Datenexportes ihre Berechtigung haben.³⁰⁹

Das Ziel der Normierung des grenzüberschreitenden Datenverkehrs liegt darin, unter Gewährung der grösstmöglichen Freiheit (gegenüber Datenschutz-Staaten)³¹⁰ die restriktiveren Institute³¹¹ für allgemein normierte Tatbestände einzusetzen. Damit wird das Postulat des freien Datenexportes verwirklicht und ein abgestufter, optimierter Persönlichkeitsschutz erreicht, wobei für den Bearbeiter im In- und Ausland durch generelle gesetzliche Bestimmungen über die Anwendbarkeit der Genehmigungsinstitute ein Zustand von Voraussehbarkeit und Rechtssicherheit geschaffen wird.

308 Export von Daten, Zugriff auf Datenbanken, Benutzung ausländischer Hard- und Software.

309 Z.B. bei multinationalen Firmen zum Austausch gesellschaftsinterner Daten mit andern verbundenen Konzernunternehmen ausserhalb des geschützten Datenraumes.

310 Das Prinzip der Reziprozität (Gegenseitigkeit) wird auch hier eine Rolle spielen.

311 Konzession, Muster- oder Einzelgenehmigung.

§ 10 BESTREBUNGEN INTERNATIONALER ORGANISATIONEN

Seit gut einer Dekade beschäftigen sich neben nationalen Kommissionen und Parlamenten auch internationale Gremien und Organisationen¹ mit der Frage des Datenschutzes. Dies aus der Erkenntnis, dass einerseits die Probleme gegenüber der computerisierten Informationsverarbeitung in allen entwickelten Ländern etwa gleichgelagert sind, andererseits aber ein multinationaler Konsensus über die Grundprinzipien des Schutzes der Privatsphäre, angesichts der durch die Telekommunikation ermöglichten Datenfernverarbeitung und DV-Systemkoppelung, entscheidende Vorteile bringen wird, sobald die Verarbeitungsvorgänge nicht mehr auf ein nationales Territorium beschränkt sind. Die rechtliche Entwicklung hat denn auch gezeigt, dass ein Konsens über grundlegende Prinzipien und einheitliches Rechtsinstrumentarium² grundsätzlich erzielt werden kann, ein Einheitsrecht aber (zur Zeit) nicht realistisch ist, sondern sich vielmehr materiell- und formellrechtliche Unterschiede zwischen den nationalen Datenschutzgesetzen ausgebildet haben.

Internationale Organisationen haben Bestrebungen unternommen zur Angleichung der nationalen Gesetze zwecks Vereinheitlichung bzw. Ausdehnung des Persönlichkeitsschutzes auf internationaler Ebene. Die Zielsetzung dieses einheitlichen Datenschutznetzes besteht nicht nur in der Verwirklichung eines optimierten Persönlichkeitsschutzes im internationalen Rahmen, sondern auch in einer Verankerung der individuellen und von der Datenverarbeitung potentiell bedrohten Grundfreiheiten im internationalen Bereich. Mit der Schaffung eines mehrstaatlichen Schutzbereiches werden aber gleichzeitig Befürchtungen über die Entstehung von schutzfreien "Oasenräumen" laut, die bewirken, dass zwischen diesen geschützten und ungeschützten Bereichen eine Zäsur gezogen wird. Diese Trennung wird über eine Steuerung der inter-

1 Europarat, OECD, Europäisches Parlament i.V. mit EG-Kommission, Nordischer Rat, IBI, Organisationen, die sich aus Entwicklungsländern konstituieren, UNESCO, UN-Menschenrechtskommission (vgl. FREESE, Data Flow, S. 58).

2 Z.B. Resolutionen (73) 22 und (74) 29 des Europarates.

nationalen Datenflüsse angestrebt, die verhindern soll, dass schutzbedürftige Informationen in "data havens" gelangen und das Schutzdispositiv der Datenschutz-Staaten unterlaufen. Innerhalb des geschützten Gebietes ist man hingegen bemüht, die Informationsflüsse zwischen den Staaten zu verbessern und die durch den Schutz des Persönlichkeitsrechts entstandenen Schranken in ihrer negativen Auswirkung auf die Industrie- und Wirtschaftspolitik möglichst gering zu halten, so dass in diesem Schutzraum ein ungehinderter Handels- und Wirtschaftsverkehr gepflegt werden kann und garantiert bleibt. Dies bedeutet nicht nur einen freien Datenverkehr unter den Staaten mit eigenem Datenschutzgesetz, sondern auch eine möglichst ungehinderte Datenkommunikation mit den Ländern, welche der betreffenden Organisation angehören, aber nicht über ein diesbezügliches Gesetzeswerk verfügen, freilich unter gleichzeitiger Wahrung des Schutzeffektes innerhalb des Interessenverbundes.

I. Die Resolutionen des Europarates

Die Resolutionen ³ des Europarates haben die erste Phase der Bemühungen dieses internationalen Gremiums zur Erreichung eines Konsenses über die für den Datenschutz grundlegendsten Prinzipien abgeschlossen. (Die Entschliessungen sind sowohl für den öffentlichen als auch privaten Bereich konzipiert und erstrecken sich somit auf alle möglichen Anwendungsgebiete eines Datenschutzrechts). Sie enthalten keine rechtssetzenden Normen, sondern sind entsprechend ihrem Zweck

-
- 3 - Resolution des Europarates an die Regierungen der Mitgliedstaaten über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im privaten Bereich:
Protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, Résolution (73) 22 adopté par le Comité des Ministres du Conseil de l'Europe le 26 septembre 1973.
- Resolution des Europarates an die Regierungen der Mitgliedstaaten über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im öffentlichen Bereich:
Protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, Résolution (74) 29 adopté par le Comité des Ministres du Conseil de l'Europe le 20 septembre 1974.

rein empfehlender Natur, was in den einzelnen Grundsätzen deutlich zum Ausdruck kommt.

Zweck dieser Entschliessung ist, Abweichungen unter den verschiedenen nationalen Datenschutzgesetzen in den Mitgliedstaaten zu vermeiden,⁴ um eine Harmonisierung⁵ auf internationaler Ebene zu vereinfachen. Aus diesem Grunde sind im Anhang zur Entschliessung eine Reihe von Grundsätzen zum Datenschutz formuliert worden, die nach Auffassung des Komitees von den Mitgliedstaaten in die in Ausarbeitung befindlichen nationalen Datenschutzgesetze oder in die bestehende Ordnung des Persönlichkeitsschutzes eingebaut werden sollen.⁶ In den bisher erlassenen Datenschutzgesetzen des europäischen Raumes sind denn auch diese Grundsätze weitgehend als Leitsätze beachtet worden, so dass die Grundstruktur der rechtlichen Instrumente des Datenschutzes in den verschiedenen Gesetzen zum grössten Teil übereinstimmt.

Die in diesen beiden Resolutionen verwirklichten Grundsätze bilden die Grundlage für den sog. "noyau dur" der Konvention⁷ des Europarates und sind darin weitgehend berücksichtigt und verwirklicht.

Einigermassen verwunderlich ist die Tatsache, dass weder im öffentlichen noch im privaten Bereich, weder in den Grundsätzen der Resolutionen, noch in den erläuternden Berichten Empfehlungen in bezug auf den grenzüberschreitenden Datenverkehr aufgestellt worden sind, obwohl dem Europarat diese Problematik bekannt war⁸ und ein Aus-

4 Resolution (73) 22: "... Considering that it is urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergencies between the laws of member States in this field; ...".

5 Resolution (73) 22, S. 10 N 4: "... it seems highly desirable that, whenever possible, common norms should be adopted in all member States, based on the idea of a 'European public order'."

6 Begründung für diese empfohlene Implementierung: "A survey, conducted in 1968-70 by the Committee of Experts on Human Rights of the Council of Europe .. has shown that the existing law does not provide sufficient protection for the citizen against intrusions on privacy by technical devices." [Resolution (73) 22 S. 9 N 2].

7 Vgl. nachfolgend, S. 250ff.

einanderklaffen der nationalen Regelungen mindestens so wahrscheinlich ist wie bei dem übrigen Datenschutzinstrumentarium; die Verabschiedung von Grundsätzen hätte auch in diesem Problemkreis das bis zum Abschluss einer Konvention⁹ bestehende Vakuum einigermaßen ausgefüllt.

Bedauerlich ist auch die Tatsache, dass diese Empfehlungen nur für natürliche und nicht auch für juristische Personen gelten: Die Auswirkungen haben sich bereits in den verschiedenen Gesetzen und Entwürfen niedergeschlagen, mit dem Resultat, dass in einem Teil der Gesetze und Entwürfe juristische Personen den Persönlichkeitsschutz genießen¹⁰ und im andern Teil noch schutzlos sind.^{11 12}

Trotz diesen beiden negativen Punkten haben diese Empfehlungen bisher ihren Sinn und Zweck erfüllt, so dass heute in Europa - soweit Datenschutzbestimmungen bestehen - eine gewisse Homogenität der Mittel vorhanden ist, was die Vereinheitlichung des Datenschutzes erleichtert. Obwohl die beiden Resolutionen für die Mitgliedstaaten des Europarates völkerrechtlich nicht verbindlich sind, ist ein in der Rechtsentwicklung interessantes Phänomen zu beobachten: Der bis jetzt durch Befolgung der Grundsätze erreichte internationale Standard ist nicht aus nationalen Rechtsordnungen herangewachsen, sondern massgeblich dem Weitblick und der Initiative internationaler Organisationen (vor allem Europarat und OECD) zu verdanken.

Nachdem die Empfehlungen des Europarates vorlagen, unternahmen drei internationale Institutionen¹³ Anstrengungen zur Lösung des

8 "Bis zum Abschluss eines etwaigen internationalen Abkommens empfiehlt das Ministerkomitee den Regierungen..." = Hinweis auf eine Konvention, in: Mitteilungsblatt der Rechtsabteilung des Europarates, April 1974. (Dies impliziert allerdings noch nicht die Kenntnis der Probleme des grenzüberschreitenden Datenverkehrs.)

9 Der Europarat beauftragte 1977 ein Expertenkomitee mit der Ausarbeitung einer Konvention, die den grenzüberschreitenden Datenverkehr zur Verstärkung des Persönlichkeitsschutzes regeln soll.

10 Z.B. in Frankreich, Oesterreich.

11 Z.B. in der BRD.

12 SCHUCAN (S. 27 Anm. 68) zitiert STEINMUELLER, der den Schutz von Personengruppen (als "Personenmehrheit" und nicht als juristische Person verstanden) bereits für wichtiger betrachtet, als den Individualschutz.

13 Europarat, OECD, und Europäisches-Parlament.

Problems des Datenschutzes im transnationalen Informationsverkehr. Diese Arbeiten haben zu drei voneinander abweichenden Vorlagen geführt, die in den nachfolgenden Ausführungen einer näheren Betrachtung unterzogen werden.

II. EUROPARAT: Datenschutz-Konvention ¹⁴

1. Vorbemerkung

Der Ministerrat des Europarates hat am 17. Sept. 1980 den Entwurf der Datenschutz-Konvention, d.h. eines "Uebereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" einschliesslich einer "Amtlichen Begründung"¹⁵ bzw. eines sog. "Rapport explicatif" genehmigt und verabschiedet. Die Konvention ist als sog. "offene Konvention" konzipiert (Art. 23) und steht demnach auch Nicht-Mitgliedstaaten des Europarates (z.B. USA, Australien, Japan etc.) zum Beitritt offen. Die Konvention bedarf aber für ihr Inkrafttreten vorerst der Unterzeichnung durch mindestens fünf Mitgliedstaaten des Europarates und wird zu diesem Zwecke ab 28. Januar 1981 zur Annahme aufliegen. Da die Konvention mit dem Rapport explicatif ausführlich kommentiert ist, beschränke ich mich auf grundlegende, kritische Anmerkungen.

2. Inhalt der Konvention

Die Konvention besteht aus drei Hauptteilen,¹⁶ denen allgemeine Bestimmungen vorgehen und am Schluss noch Verfahrens- und Vollzugsnormen beigelegt sind (Art. 18-27).

A. Präambel und allgemeine Bestimmungen

a) Präambel

In der Präambel sind drei Grundsätze verankert, zu deren Einhaltung sich die Signatarstaaten verpflichten:

- Die Wahrung der Grundrechte ¹⁷ (Menschenrechte und Grundfreihei-

14 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, in: série des traités européens, No. 108.

15 Vgl. AUERNHAMMER, DS+DS 4/80, S. 181f.

16 CONSEIL DE L'EUROPE, Rapport explicatif, N 18.

ten), insbesondere der Persönlichkeitsrechte beim Austausch personenbezogener Daten über die Landesgrenzen hinweg.

- Die Beachtung und Aufrechterhaltung des Prinzips der Informationsfreiheit.¹⁸
- Die Notwendigkeit eines Ausgleichs der Grundwerte von Datenschutz als Ausdruck des Persönlichkeitsschutzes und dem freien Informationsfluss als Ausdruck der Informationsfreiheit.

Die Orientierung an den Grundrechten der EMRK scheint mir einen guten Ausgangspunkt zu bilden.¹⁹ Dementsprechend wird besonders viel Gewicht auf die Verwirklichung des ersten Postulates gelegt, währenddessen den einzelnen Gesetzgebern keine Hinweise gegeben werden, wie der Ausgleich des Spannungsverhältnisses von Datenschutz und freiem Informationsfluss bzw. Informationsfreiheit zu vollziehen ist. Die Lösung dieser schwierigen Aufgabe bleibt denn auch in der Konvention weitgehend unbeantwortet, so dass die Grundsätze II und III nur im Kontext des Persönlichkeitsschutzes behandelt werden und keine nähere Bestimmung erfahren. So fehlt, wie erwähnt, bezüglich der Informationsfreiheit eine Aussage und Abgrenzung, die das Recht auf Daten näher umreißt und dabei auch eine Lösung der diametral entgegengesetzten Anforderung zum Schutz vor Daten gibt.

Die Präambel enthält in ihrem Wortlaut ausserdem zwei grundlegende und bedeutende Einschränkungen:²⁰

- Beschränkung des Anwendungsbereiches auf automatisierte Verarbeitungsvorgänge und
- Begrenzung des Schutzes der Persönlichkeitsrechte und Grundfreiheiten auf natürliche Personen.

b) Zweck²¹

In der Umschreibung des Zweckes wird nochmals die Beschränkung

17 Vgl. Art. 8 EMRK.

18 Vgl. Art. 10 EMRK.

19 Dieser Lösungsansatz hat allerdings den Einbezug der juristischen Personen, Vereinigungen und Personengruppen etc. in den Rahmen des von der Konvention gewährleisteten Schutzes verhindert.

20 Auf sie wird in der folgenden Besprechung nochmals einzugehen sein.

des Schutzes auf die natürlichen Personen erwähnt; dabei werden aber die in der Präambel erwähnten Grundsätze nicht mehr zum Gegenstand des Zweckartikels erhoben.

Die Gleichstellung und Gleichbehandlung von In- und Ausländern beim Persönlichkeitsschutz ist eine Absage an die von einigen Staaten²² gemachte Unterscheidung zwischen Staatsangehörigen bzw. Fremden mit Wohnsitzgenehmigung und Ausländern - eine nationale Norm dieser Art würde dem Konventionsziel klar zuwiderlaufen.

Die generelle Fassung dieser Bestimmung - auch auf Personen von Nichtmitgliedstaaten - ist ein hochgestecktes Ziel, dessen Verwirklichung bei kollisionsrechtlichen Fragen u.U. zum Herd weiterer, nur schwer lösbarer Anknüpfungsprobleme²³ werden kann. M.E. wäre diesfalls auch notwendig, dass die Konvention eine konkrete Lösung zu den Kollisionsproblemen gibt, die durch die Gleichstellung von In- und Ausländern bei international verknüpften Tatbeständen resultieren.

Die hier nochmals aufgeführte Beschränkung des Anwendungsbereiches auf den Schutz der Privatsphäre gegenüber der automatisierten Datenverarbeitung kann zu einer - von Verarbeitungsvorgängen abhängigen - differenzierten Behandlung der Privatsphäre und des Persönlichkeitsrechtes in den einzelnen nationalen Rechtskreisen führen.

c) Definitionen²⁴

aa) Die Beschränkung des Schutzbereiches auf personenbezogene Daten natürlicher Personen vermittelt einerseits einen bloss partiellen Schutz und eröffnet andererseits auch Umgehungsmöglichkeiten:

- Fragmentarisch ist der Schutz, weil eine rechtliche Ungleichbehandlung gleichwertiger wirtschaftlicher Interessen erfolgt.²⁵
- Personenbezogene Daten können leicht als Firmendaten gespeichert werden, da in vielen Fällen Gesellschaft und Benützer identisch sind, so dass eine Grauzone entsteht.

21 Art. 1 KE.

22 Z.B. USA, CDN.

23 Vgl. hinten, S. 268.

24 Art. 2 KE.

- Es ergeben sich Abgrenzungsprobleme in dem Falle, wo jemand als legitimierte Einzelperson Individualrechte ausüben will und diese ihm nicht gewährt werden, weil er vom Auskunftgebenden u.U. als nicht legitimierter Vertreter bzw. Organ einer juristischen Person oder Personengruppe behandelt wird.
- Es erfordert eine kaum vollziehbare, unterschiedliche Behandlung von gleichen Datenarten innerhalb einer Datenbank oder eines Verarbeitungsprozesses: Wie können personenbezogene Daten juristischer Personen (z.B. eine Einmann-AG betreffend) oder von Personengruppen von denjenigen natürlicher Personen bezüglich der automatisierten Verarbeitungsvorgänge differenziert werden?
- Im internationalen Bereich ist der Schutz juristischer Personen speziell angebracht, um einerseits gewisse staatliche Eingriffe in Form von Kontroll- bzw. Einsichtsrechten zu verhindern und andererseits die im privaten marktwirtschaftlichen Sektor stets drohende Verletzung von Persönlichkeitsrechten mit ihren weitreichenden Auswirkungen zu unterbinden. Ausserdem werden die juristische Personen (d.h. [multi-]nationale Gesellschaften) betreffenden Informationen den Grossteil der transferierten personenbezogenen Angaben darstellen, so dass deren Schutzbedürftigkeit m.E. einer genaueren Analyse bedarf, bevor eine generelle Ausklammerung dieser Datenkategorie erfolgt.

Eine allgemeine Beschränkung des Schutzbereiches hat innerhalb der Konvention auch eine gewisse Signalwirkung auf die zukünftige Rechtsfortbildung in legiferierenden oder novellierenden Staaten, so dass mit einer generellen Ausklammerung der juristischen Person der zum Gegenstand der Konvention gemachte Zweck der Stärkung des Schutzes der Daten von Individuen ²⁶ m.E. nicht erfüllt wird. Die umgekehrte Vorgehensweise, die einen umfassenden Schutz für juristische und natürliche Personen, Personengruppen sowie Vereinigungen

25 Z.B. bei gleichem Zweck ist der Einzelkaufmann hinsichtlich der Kontrollrechte besser gestellt als der Alleinaktionär der Einmann AG).

26 CONSEIL DE L' EUROPE, Rapport explicatif, N 1.

von Personen vorsieht und eine Beschränkung des Schutzes auf natürliche Personen durch den nationalen Gesetzgeber erlaubt, wäre ein alternatives Konzept.

bb) Gegenstand des Schutzes bilden personenbezogene Daten oder Datensätze, die Objekt einer automatisierten Bearbeitung darstellen. Damit werden nicht nur zentralisierte Datenbestände, sondern auch geographisch zerstreut liegende Daten erfasst, die zwecks Verarbeitung über Computerverbindungen in einem zentralen System kombiniert werden können.²⁷

In den Anwendungsbereich fallen aber nur Daten, die in automatisierten Vorgängen verarbeitet werden, so dass ein wichtiger Teil des gesamten personenbezogenen Datenbestandes im Bereich der manuellen Verarbeitungsschritte nicht vom "Konventionsschutz" profitieren kann. Folgende Überlegungen sprechen grundsätzlich für einen Einbezug von Daten, die manuell bearbeitet wurden:

- Im Rahmen der automatisierten Datenverarbeitung lassen sich nicht alle Bearbeitungsvorgänge auf automationsunterstützte Weise vollziehen,²⁸ vielmehr bleiben all diejenigen Daten, die des automatisiert-verarbeiteten Charakters entbehren, vom Schutz ausgenommen, so dass ein Datum nicht während aller Verarbeitungsvorgänge, denen es unterworfen ist, geschützt bleibt. Es fehlt ein umfassender Schutz, denn ein manuell erstellter Informationsträger (z.B. Formular) kann auch vor bzw. unabhängig von einer automatisierten Verarbeitung die Ursache einer Persönlichkeitsverletzung darstellen. Schon die bloße Existenz eines manuell ausgefüllten Erhebungsblattes ist eine Gefährdung der Privatsphäre, nicht erst die automatisierte Verarbeitung dieser Daten.
- Soll der von einem nationalen Gesetz bzw. internationalen Konvention verliehene Schutz bezüglich der Datenverarbeitung umfassend sein, müssen zumindest all diejenigen Daten in den Anwendungsbereich fallen, die im Konnex mit einer vorangegangenen bzw. nachfolgenden automatisierten Verarbeitungshandlung auf manuelle Weise bearbeitet wurden.²⁹

27 Id., a.a.O., N 1.

Für das weitergehende Postulat, die Daten unter allen manuellen oder automatisierten Bearbeitungsverfahren - ohne das Erfordernis der Verknüpfung mit einem automatisierten Vorgang - dem Schutz zu unterstellen, sprechen folgende Argumente:

- Die Beschränkung des Schutzes auf automatisiert verarbeitete Daten, kann zu einer wirtschaftlichen Diskriminierung gewisser moderner Technologien führen, vor allem, wenn ein nationales Gesetz die Errichtung automatischer Informationssysteme an sehr restriktive Voraussetzungen knüpft.
- Diskriminierungen können ihren Ursprung aber auch darin haben, dass staatliche oder private Körperschaften, die infolge der gemäss Aufgabenkreis oder Funktion zu bewältigenden Datenmenge und durchzuführenden Verarbeitungsvorgänge gezwungen sind, sich automatisierter Verfahren zu bedienen, einer strengerer Regelung unterworfen werden, als jene Stellen, die sich für ähnliche Aufgaben der manuellen Verarbeitung bedienen, obwohl die bearbeiteten Daten für das Datensubjekt eine ähnliche Gefährdung der Persönlichkeit darstellen und nach einem entsprechenden Schutz rufen, wie diejenigen der automatisierten Verarbeitung.³⁰
- Die Beschränkung auf die automatisierten Verarbeitungsphasen hat auch zur Folge, dass sich Umgehungsmöglichkeiten durch eine Verlagerung der automatisierten auf manuelle Bearbeitungsvorgänge eröffnen, wenn die Informationen dem Schutz eines Gesetzes entzogen werden sollen.³¹ Diese enge Fassung der geschützten Verarbeitungs-

28 Z.B. Ausfüllen von maschinenlesbaren Formularen.

29 Vgl. österreichisches Modell, vorne, S. 165f.

30 Es ist längst bekannt und unbestritten, dass manuell bearbeitete Datensammlungen ebenso die Persönlichkeit zu verletzen vermögen wie automatisiert verwaltete; aus dieser Tatsache folgt, dass auch für Angaben die manuell verarbeitet werden, adäquate Sicherungsvorkehrungen ergriffen werden müssen, wobei die spezielle Eigenart der Verarbeitungsweise in der rechtlichen Regelung ihren Niederschlag finden muss.

31 Wollte man dem gesetzlichen Schutz entgehen, könnte man z.B. dem gesetzlichen Anwendungsbereich unterstehende Datensammlungen in einen andern Vertragsstaat exportieren, der entsprechend der Konvention nur automatisiert verarbeitete Angaben schützt, und sie dort in eine nicht-automatisierte Form umsetzen.

arten bzw. Daten bildet, ähnlich wie der eingeschränkte Schutzbereich, Grundlage für national unterschiedliche Ausgestaltungen fundamentaler Fragen.³²

cc) Die in Art. 2 lit. c aufgeführte Fassung der möglichen Verarbeitungsschritte erscheint mir zu eng, da sie die Bearbeitungsverfahren enumeriert ("opérations suivantes" bzw. "following operations") und nicht als Beispiele weiterer und zukünftiger Vorgänge aufführt.

Die im Rapport explicatif³³ erwähnte Ausklammerung des Sammelns von Daten vom Begriff der Verarbeitung bedarf einer näheren Umschreibung,³⁴ damit eine Subsumtion bzw. Einordnung neuer Verarbeitungsmethoden im bestehenden Schutzsystem erfolgen kann. Der grundsätzliche Ausschluss des Sammelns von Daten vom Begriff der Verarbeitung muss in der KE im Zusammenhang mit Art. 5 lit. a und i.V. mit Art. 12 betrachtet werden.³⁵

dd) Die Bezeichnung einer verantwortlichen Stelle betrifft gemäss Rapport explicatif³⁶ diejenige Stelle, die für Festsetzung des Zweckes der ADV verantwortlich ist und überdies bestimmt, welche Daten gespeichert und welchen Verarbeitungsvorgängen sie unterzogen werden.

32 Die Einigung auf dem kleinsten gemeinsamen Nenner hat auch hier auf die Rechtsfortbildung einen negativ präjudizierenden Einfluss.

33 A.a.O., N 31.

34 So ist nicht klar, ob unter dem Begriff "la collecte d'information" nur das Sammeln oder auch das Erfassen von Daten verstanden wird. Diese Abgrenzung kann von Bedeutung sein, wenn auch das Erfassen automatisiert vollzogen wird, z.B. durch "optical readers", "scanners" etc., die normal lesbare Handschriften zu erfassen vermögen, die von ihrem Urheber nicht für eine spätere automationsunterstützte Verarbeitung gedacht und vorgesehen waren (z.B. bei Aufnahme von Korrespondenz). Die zukünftige Technologie wird aber auch die sprachaktivierte Eingabe zur Textverarbeitung oder Informationsspeicherung (vgl. IBM, NZZ Nr. 180/1980, S. 37) sowie die Bilderfassung ermöglichen: Hinsichtlich dieser Aussichten hat eine Begriffs Umschreibung Auskunft zu geben.

35 Vgl. hinten, S. 257ff.

36 A.a.O., N 32.

Die Verantwortung für die Einhaltung eines Gesetzes und die Haftbarkeit gegenüber Ansprüchen Dritter folgt nicht direkt aus der entsprechenden Bestimmung, sondern aus dem Inhalt des Art. 8 KE. Ueber die obligatorische Bezeichnung einer verantwortlichen Stelle gibt die KE keine eindeutige Antwort, eine solche kann nur aus Art. 2 lit. d i.V. mit Art. 8 lit. c gefolgert werden. Aus dieser wenig präzisen Umschreibung können Abgrenzungsprobleme bei einem Lastverbund oder sog. integrierten Datenverarbeitungssystemen hinsichtlich der erforderlichen Bezeichnung einer verantwortlichen Stelle resultieren, vor allem, wenn mehrere derartige Stellen möglich sind und die nationalen Gesetze verschiedene Kriterien für deren Identifikation anwenden.

d) Beschränkungs- und Ausdehnungsmöglichkeit des Anwendungsbereiches

aa) Beschränkung des Anwendungsbereiches ³⁷

Vom Anwendungsbereich einer Konvention können nur jene automatisiert verarbeiteten Datenkategorien ausgenommen werden, die nicht dem Schutz des nationalen Gesetzes unterstellt sind. Die Beschränkung ist eine logische Folge der nationalstaatlich unterschiedlichen Anwendungsspektren. Die Einschränkungsmöglichkeit auf natürliche Personen, wie sie in dieser Norm der Konvention vorgesehen ist, kann Probleme mit sich bringen, da diese Sollbruchstellen nicht nur die territoriale Datenoasenbildung fördern, sondern sogar schutzfreie Verarbeitungsräume in einzelnen Vertragsstaaten schaffen und Grundlage für sog. "Convention havens" bilden.

bb) Ausdehnung des Anwendungsbereiches ³⁸

Die Ausdehnungsmöglichkeit "spiegelt in selten deutlicher Weise die Verwirrung auf der internationalen Datenschutzszene wider."³⁹ Obwohl in Präambel, Zweckartikel und den Definitionen der Schutz nur

37 Art. 3 Abs. 2 lit. a KE.

38 Art. 3 Abs. 2 lit. b/c KE.

39 MEISTER, DS+DS 1/80, S. 13.

auf personenbezogene Daten natürlicher Personen durch die ADV beschränkt wurde, eröffnet lit. b die Möglichkeit der Ausdehnung auf juristische Personen, Personengruppen, Vereinigungen mit oder ohne Rechtspersönlichkeit und lit. c auf manuellen Verarbeitungsvorgängen unterstellte Daten.

Damit bildet die Wahl des kleinsten gemeinsamen Nenners zur Bestimmung des Anwendungsbereiches einen Ansatzpunkt für nationale Abweichungen vielfacher Art, die dem in der Konvention verankerten Sinn der Angleichung der Rechte der Mitgliedstaaten nicht unbedingt förderlich ist.

B. Bestimmung des materiellen Rechts in Form von Grundprinzipien

Als zentraler Teil der Konvention gilt Kapitel II., das die Grundprinzipien des Datenschutzes beinhaltet.⁴⁰ Zweck dieser Prinzipien ist es, einen gewissen Mindestschutz-Standard für die automatisierte Datenverarbeitung sicherzustellen und mittels einer Ueberführung dieses "noyau dur" in die nationale Gesetzgebung der Signatarstaaten eine möglichst einheitliche Entwicklung des Datenschutzrechts in den Mitgliedsländern zu erreichen. Letztlich soll die einheitliche Ausprägung des Datenschutzes bestehende Hindernisse oder protektionistische Schranken des grenzüberschreitenden Datenverkehrs abbauen und das Prinzip des freien Informationsflusses verwirklichen helfen. Ausserdem soll die durch den noyau dur angestrebte Harmonisierung der nationalen Gesetze dazu beitragen, potentielle Probleme des anwendbaren Rechts und Fragen des zuständigen Forums zu vermeiden.

Sicherlich wird durch den noyau dur eine gewisse Rechtsvereinheitlichung erzielt; deren Bedeutung liegt m.E. jedoch vorab im Aufbau eines gegenseitigen Vertrauens in das Schutzvermögen der Datenschutzgesetzgebung der Vertragsstaaten und ist demzufolge für den Abbau von Datenhindernissen und den freien Informationsfluss sicherlich unerlässlich. Hingegen ist zu bezweifeln, dass sich dadurch auch

40 CONSEIL DE L' EUROPE, Rapport explicatif, N 20.

die Probleme des anwendbaren Rechts und die Frage der örtlichen und sachlichen Zuständigkeit eliminieren lassen. Es ist zudem fraglich, ob die Einigung auf eine "Minimalausrüstung" an Datenschutz mit zahlreichen nationalen Abweichungsmöglichkeiten eine taugliche Lösung für die schwierig zu meisternden Probleme des anwendbaren Rechts, des zuständigen Forums, der Regelung der internationalen Datenflüsse und des Ausgleichs der widerstrebenden Interessen von Informationsfreiheit und Datenschutz darstellt.

a) Ueberführung der Prinzipien ins nationale Recht

Die Ueberführung dieser Prinzipien ins nationale Recht ist deshalb notwendig, weil die Konvention als "non self-executing Convention" konzipiert ist, d.h. dass aus ihr direkt keine Rechte geltend gemacht werden können und deshalb für die Wirksamkeit dieser Grundprinzipien ihre Uebernahme in das nationale Recht erforderlich ist. Die Art und Weise der Ueberführung der Prinzipien des noyau dur ins nationale Recht, d.h. deren Umsetzung in konkrete materielle Datenschutznormen, wird jedem Mitglied überlassen.

b) Grundprinzipien

Die im noyau dur aufgestellten Grundprinzipien entsprechen weitgehend denjenigen der beiden Europarat-Resolutionen.^{41 42}

aa) Qualität der Daten⁴³

Der bewusste Verzicht⁴⁴ auf eine weitere differenzierte Behandlung zwischen öffentlichem und privatem Bereich wegen möglicher unterschiedlicher Auffassung dieser Begriffe in den Vertragsstaaten, wirkt sich negativ auf den privaten Sektor aus, da als Ausgangspunkt das Modell des Datenschutzes im öffentlichen Bereich diente. Dies ist umso bedauerlicher, als die in den Resolutionen getrennt behandelten Prinzipien in der Konvention zugunsten eines gemeinsamen Nenners auf

41 Resolutionen (73) 22 und (74) 29.

42 CONSEIL DE L' EUROPE, Rapport explicatif, N 40.

43 Art. 5 KE.

44 CONSEIL DE L' EUROPE, a.a.O., N 33.

eine einheitliche Formulierung gebracht wurden; damit wird aber den Bedürfnissen des privaten Bereichs auf eine relativierte Anwendung der für den öffentlichen Sektor geltenden Grundsätze in der Konvention nicht nachgekommen. So ist z.B. im privaten Bereich der Verarbeitungszweck nicht so genau determinierbar wie bei der vom Legalitätsprinzip beherrschten öffentlichen Verwaltung. Ebenso können die nicht relativierten Forderungen nach Exaktheit und Aktualität der Daten, die im Bereich der öffentlichen Eingriffsverwaltung durchaus angemessen sind, im privaten Sektor kontraproduktiv wirken, da sie zu dauernder inquisitorischer Nachforschung nach Veränderung im Bestand personenbezogener Angaben zwingen und dabei nicht nur die Tätigkeit der datenverarbeitenden Stellen, sondern auch die von einer Speicherung betroffenen Personen stark belasten. Eine Relativierung der Pflicht zur Nachführung und Korrektheit der Daten auf einen Status, der den Bedürfnissen des konkreten Verarbeitungszweckes entspricht, würde negative Auswirkungen vermeiden helfen. Auch hinsichtlich der Speicherdauer wären relativierte Anforderungen für den privaten Bereich zweckmässig, so dass für die materielle Qualität der Daten eine gegenüber dem öffentlichen Bereich grundsätzlich differenzierte Behandlung als angebracht erscheint.

bb) Spezielle Datenkategorien ⁴⁵

Für Datenkategorien, die sog. sensitive Informationen enthalten, ist angesichts der damit verbundenen erhöhten Gefährdung des Persönlichkeitsrechts eine automatisierte Verarbeitung nur im dem Rahmen erlaubt, als das nationale Recht geeignete Schutzvorkehrungen ⁴⁶ enthält.

Die nicht abschliessende Aufzählung der Datenkategorien ermöglicht eine Abstufung der Sensitivität von Daten in den nationalen Datenschutzgesetzen entsprechend dem soziologischen Kontext des Mitgliedsstaates.

⁴⁵ Art. 6 KE.

⁴⁶ Darunter fallen nicht nur die Gesetzgebung, sondern auch spezielle Bestimmungen, behördliche Verordnungen und Verfügungen.

Die aus den Definitionen folgende Beschränkung auf die automatisierte Verarbeitung sowie die Ausklammerung des Sammelns von Daten kann sich dabei negativ auswirken, vor allem weil damit die Sammlung oder manuelle Verarbeitung sensibler Information gemäss noyau dur erlaubt ist und das nationale Recht keine geeigneten Sicherungsvorkehrungen aufweist. Hier stellt sich die Frage, welche Wirksamkeit dem noyau dur zukommt, wenn Umgehungsmöglichkeiten derart offenkundig sind.

cc) Datensicherung ⁴⁷

Die Konvention gewährt einen Schutzbereich, in dem die Sicherungsmassnahmen die entscheidenden Schutzkriterien und die Angemessenheit der Mittel gegenüber bestimmten Verarbeitungsvorgängen wie auch gegenüber der durch die Datenverarbeitung für das Datensubjekt bestehenden Risiken zu erfüllen vermögen. Ausserdem sollen die Datensicherungsbestimmungen angemessen und realisierbar hinsichtlich der mit diesen Sicherungsvorkehrungen verbundenen Kostenlast sein;⁴⁸ gegenüber neuen Technologien und Verarbeitungsmodalitäten sollen die Massnahmen flexibel und wirksam angepasst werden können.

dd) Zusätzliche Schutzmassnahmen ⁴⁹

Die hier spezifizierten Schutzmassnahmen sollen dem Datensubjekt die Möglichkeit geben, seine Rechte gegenüber der ADV durchzusetzen; der Inhalt des Art. 8 entspricht klar den in den nationalen Rechten institutionalisierten Individualrechten.⁵⁰

Einzelne Vorschriften (lit. a) entbehren einer klaren Funktionsbestimmung und materiellen Ausgestaltung, die aufzeigen würde, wie z.B. die Festlegung des Sitzes einer verantwortlichen Stelle zu geschehen hat, falls bei einem integrierten Datennetz (über mehrere Staaten) eine Koppelung von selbständigen DV-Systemen erfolgt. Mit

47 Art. 7 KE.

48 Vgl. MUTTER, S. 97ff. und 123ff.

49 Art. 8 KE.

50 CONSEIL DE L' EUROPE, Rapport explicatif, N 50.

welcher materiellen Vorschrift wird sichergestellt, dass bei einem Informationssystem-Verbund tatsächlich eine verantwortliche Stelle in einem der Vertragsstaaten liegt oder eine bloss deklaratorische Sitzbestimmung vermieden wird? Eine materielle Bestimmung dieser Art ist unerlässlich, wenn die Konvention eine klare Angabe der verantwortlichen Stelle bezweckt.⁵¹

Auch der in lit. a vorgeschriebene Publizitätsgrundsatz sollte für den privaten Bereich relativiert werden, da die totale Offenlegung der im privaten Sektor stattfindenden Datenverarbeitungen (Art von Daten, deren Zweckverwendung, Herkunft und existierenden Datensammlungen) u.U. negative Auswirkungen auf die Wettbewerbsbeziehungen haben kann und ausserdem mit dem Prinzip des Geschäftsgeheimnisses nicht vereinbar ist. Der Publizitätsgrundsatz widerspricht in dieser undifferenzierten Form dem Grundsatz der Wettbewerbsneutralität des Datenschutzes, wie er auch indirekt aus der Präambel folgt.

Die fehlende Trennung zwischen dem öffentlichen und privaten Bereich wird auch bei der Kostenfrage (lit. b) deutlich: So darf für Datensammlungen der öffentlichen Verwaltung vom Prinzip der Unentgeltlichkeit oder einer (nicht kostendeckenden) Verwaltungsgebühr ausgegangen werden. Eine analoge Anwendung dieses Grundsatzes im privaten Bereich hätte zur Folge, dass die Datenverarbeiter mit erheblichen Kosten (z.B. durch kostenlose oder nicht kostendeckende Auskunftserteilung) belastet werden könnten, sei es dass spezielle Suchprogramme erstellt werden müssten oder u.U. sogar eine Reorganisation der Datenbank notwendig würde.

Ausserdem ist auch eine Löschung, Korrektur oder Sperrung von Daten im privaten Bereich nach andern Kriterien zu beurteilen als im öffentlichen Sektor, da in der Privatwirtschaft regelmässig eine Abwägung der miteinander konkurrierenden Interessen erfolgen muss.

Die Vorschrift, dass im Falle einer durchgeführten Berichtigung von Daten nach lit. c im nationalen Recht Vorkehrungen zur Weiterlei-

51 Wie dies im Rapport explicatif (N 51) aufgeführt ist.

tung solcher Korrekturen an die Empfänger der ursprünglichen Informationen zu treffen sind,⁵² veranschaulicht die mangelnde internationale Dimension dieser Konvention aufgrund ihrer Konzeption - hier wäre eine materielle Vorschrift angebracht, die eine Weiterleitungspflicht auch an die Empfänger im Ausland vorschreibt. Eine Bestimmung dieser Art ist allein über eine Konvention mit direkter Rechtswirkung zu erreichen und hat auf einzelstaatlicher Ebene nur beschränkte Wirkung.

ee) Ausnahmen und Einschränkungen zum Datenschutz⁵³

Ausnahmen von den Grundprinzipien des Datenschutzes sind nur in dem Ausmass zulässig, als sie für den Schutz der fundamentalen Rechte einer demokratischen Gesellschaft notwendig sind.⁵⁴ Die nach dem Vorbild der Art. 8 und 10 EMRK gestaltete Ausnahme geht aber mit dem unbestimmten Begriff der "intérêts monétaires" (Währungsinteressen) weiter als die EMRK. Der Begriff verdient eine nähere Umschreibung und Präzisierung seines Inhaltes, da er denjenigen der "intérêts fiscaux" einer früheren Fassung eines VE ersetzt und nicht völlig ausgeschlossen ist, dass immer noch ähnliche Absichten hinter dem Begriff verborgen sind, obwohl der Rapport explicatif⁵⁵ darunter die sog. "exigences du recouvrement de l'impôt" sowie die "contrôles de changes", d.h. Anforderungen für den Einzug von Steuern sowie Devisen- bzw. Wechselkontrollen, verstanden haben will. Auch diese Begriffe sind in vielen Richtungen interpretierbar. Fraglich ist in diesem Zusammenhang, ob diese Begriffe die Forderung nach Vermeidung von nicht-tariflichen Datenbarrieren erfüllen.

Das in lit. b aufgeführte Geschäfts- und Unternehmensgeheimnis⁵⁶ berücksichtigt die unterschiedliche Behandlung des privaten

52 CONSEIL DE L' EUROPE, Rapport explicatif, N 54.

53 Art. 9 KE.

54 Vgl. CONSEIL DE L'EUROPE, a.a.O., N 55.

55 Id., a.a.O., N 57.

56 Davon ausgehend, dass mit "droits et libertés d'autrui" auch die Geschäftsgeheimnisse Dritter, einschliesslich der verantwortlichen Stelle, zu verstehen sind.

Bereichs gegenüber der öffentlichen Verwaltung und könnte auch Grundlage für eine Beschränkung der Einsichtsrechte gegenüber juristischen Personen bilden, falls diese ebenfalls dem Schutz unterstellt werden. Wichtig ist, dass hier eine Interessenabwägung stattfindet und dadurch ausgeschlossen wird, dass der wirtschaftlich Stärkere die Ansprüche aus dem Datenschutz gegenüber der wirtschaftlich schwächeren Partei als Waffe benutzt.

Das Zurücktreten der Individualrechte gegenüber risikolosen Verarbeitungen bei statistischen Arbeiten und wissenschaftlicher Forschung sollte keine Probleme ergeben.

gg) Ausdehnung des Schutzes⁵⁷

Die Ausdehnung des Schutzes über das im Noyau nur verwirklichte Mindestmass hinaus ist nach dieser Vorschrift in jeder Beziehung möglich. Den Vertragsstaaten wird die Schaffung eines restriktiveren Schutzsystems zugestanden, das letztlich auf die Vereitelung des freien Datenflusses und der Informationsfreiheit hinauslaufen kann, weil die Bestimmung keine Beschränkung hinsichtlich eines Ausgleichs dieser Interessensgegensätze enthält; damit bedeutet diese Ausdehnungsmöglichkeit aber gleichzeitig eine Gefahr der Verletzung der in der Präambel statuierten Grundsätze.

Ferner kann dadurch eine ungleiche Regelungsdichte zwischen den Signatarstaaten entstehen, mit der Folge einer Datenoasenbildung innerhalb des Konventionsgebietes; solche "Convention havens" provozieren v.a. die privaten Datenverarbeiter zu einer Verlagerung der Datenverarbeitungshandlungen aus einem Vertragsstaat mit einer restriktiven Gesetzgebung in einen andern mit einem liberalen Regelungswerk.⁵⁸ Das Vermeiden einer Verschiebung von Datenbanken und Datenflüssen aufgrund unterschiedlich strenger Datenschutzbestimmungen ist aber m.E. ein unausgesprochener Grundsatz der Konvention.

⁵⁷ Art. 11 KE.

⁵⁸ Vgl. nachfolgend, S. 259, Ausführungen zu Art. 12 Abs. 3.

Diese Bestimmung könnte dazu führen, dass die mit dem noyau dur beabsichtigte Angleichung der Rechte in den Signatarstaaten in Frage gestellt wird.

C. Spezielle Regeln zum grenzüberschreitenden Datenverkehr

Da es Zweck und Ziel der Konvention ist, die Grundrechte, insbesondere das Persönlichkeitsrecht beim grenzüberschreitenden Datenverkehr sowie das Prinzip der Informationsfreiheit zu wahren und einen Ausgleich der Antinomie von "Datenschutz und Informationsfreiheit" zu bringen, stellt Art. 12 über den grenzüberschreitenden Datenverkehr eine der Schlüsselbestimmungen dieser Konvention dar. Abs. 1 spezifiziert einen breiten Anwendungsbereich von Datenübertragungsarten der sowohl automatisierte als auch manuelle Uebermittlungsmethoden beinhaltet: Ein weites Spektrum von Ausprägungen des transnationalen Datenverkehrs fällt somit unter diese Vorschrift.⁵⁹ Besonders erwähnenswert ist der Einbezug des Sammelns⁶⁰ von Daten: Die Ausdehnung des Anwendungsbereiches von Art. 12 auf diesen Verarbeitungsvorgang gilt als Ausnahme zu der in den Definitionen gemachten grundsätzlichen Ausklammerung und erschien notwendig, um Umgehungsmöglichkeiten⁶¹ der Gesetze auszuschalten. Somit fällt jedes Sammeln von Daten und

-
- 59 - Erscheinungsform der Daten: Klartext, verschlüsselter Text.
- Speichermedium: Papier, Lochkarten, Lochstreifen, Magnetband, Plattenspeicher etc.
- Transportarten: physischer Transport, Post, Fernmeldeverbindungen, Satellit.
- Verbindungsart: Terminal - Computer,
Computer - Computer,
manuell - Computer.
- Nachfolgender Uebertragungskreis: direkt von Ursprungsland in Empfängerland oder indirekt über eines oder mehrere Transitländer.
- Verhältnis zwischen Sender und Empfänger: innerhalb einer Gesellschaft oder zwischen zwei verschiedenen Rechtssubjekten.
- 60 CONSEIL DE L' EUROPE, Rapport explicatif, N 64.
- 61 Umgehungsmöglichkeiten würden durch den Ausschluss des Begriffes des Sammelns (Art. 2 lit. c) insofern eröffnet, als Daten, die in einem Land erfasst und in einem andern verarbeitet werden, den Konventionsbestimmungen zu entziehen vermögen.

jede Verarbeitungsart unter den Art. 12, falls personenbezogene Angaben den bisherigen Rechtsbereich zum Zweck der automatisierten Datenverarbeitung verlassen.

Abs. 2 bildet den Kern der Konvention und enthält den Grundsatz, dass kein Mitgliedstaat gegenüber andern Vertragsstaaten unter dem Vorwand des Datenschutzes einschränkende Bedingungen (z.B. in Form von Genehmigungen) oder generelle Verbote hinsichtlich des grenzüberschreitenden Datenverkehr aufstellen darf.⁶² Allerdings ist die enge Formulierung, die das Verbot der Errichtung von Schranken auf den Zweck des Datenschutzes beschränkt, nicht dazu angetan, Hindernisse, die mit anderer Begründung vorgebracht werden und auf verborgene Weise protektionistischen Zwecken dienen, abzuwehren, so dass Datenbarrieren weiterhin errichtet werden können. Mit dieser Formulierung kann also der Grundsatz des freien internationalen Informationsflusses, wie er in der Präambel ausgesprochen wird, nicht voll verwirklicht werden.

Das grundsätzliche Verbot der Errichtung von Schranken und Hindernissen beruht auf dem minimalen Schutzstandard, den alle Mitgliedstaaten durch die Realisierung des *noyau dur* in den nationalen Datenschutzgesetzen gewährleisten.

Art. 12 verbietet nur Schranken, nicht aber Massnahmen, die es einem Staat ermöglichen, sich über den Datentransfer von seinem Territorium in das von Vertragsstaaten mittels einfacher Exportdeklarationen durch die verantwortliche Stelle zu informieren. Allerdings muss sichergestellt werden, dass diese Informationstätigkeit öffentlicher Behörden nicht zu Kontrollzwecken ausgenutzt wird und sich letztlich als nicht tarifliches Hindernis auf den transnationalen Datenfluss auswirkt.

62 Gemäss Rapport explicatif (N 67) bringt diese Formulierung eine klare Aussage, dass sich ein Vertragsstaat nicht auf diese Konvention berufen kann, um Beeinträchtigungen des grenzüberschreitenden Datenverkehrs aus Gründen, die nicht den Schutz der Persönlichkeit betreffen, zu rechtfertigen. Die einzelnen Vertragsstaaten können aber in ihrer nationalen Gesetzgebung Vorschriften schaffen, die im Einzelfall die Uebermittlung personenbezogener Daten generell (d.h. innerhalb oder ausserhalb des Staatsgebietes) untersagen (AUERNHAMMER, DS+DS 4/80, S. 180).

Die KE stellt nur eine freie, ungehinderte Datenausfuhr sicher, erwähnt dabei aber nicht den Fall des Importes bzw. des Wiederimportes. Im Zusammenhang mit einem freien Export ist die Frage des Wiederimportes von Bedeutung, wenn die freie Ausfuhr dazu benützt wird, bestimmte, nach dem Datenschutzrecht des Ursprungs- bzw. Exportlandes nicht gestattete Verarbeitungsschritte in einem andern Vertragsstaat durchzuführen und danach die Daten ins Ursprungsland zu reimportieren. Da keine Bestimmung statuiert wurde, die einen freien Import garantiert, können die Vertragsstaaten den Eintritt von Daten, die aus einem andern Land stammen oder wiederimportiert werden, mühe-los einer vorhergehenden speziellen Genehmigung unterwerfen. Da Import und Export komplementär sind, d.h. sich gegenseitig bedingen, ist mit der blossen Forderung nach einem Verbot der Exportgenehmigung und einer fehlenden gleichlautenden Bestimmung zum Import das Postulat und Prinzip des freien grenzüberschreitenden Datenverkehrs keineswegs ganz erfüllt.

Abs. 3 ermöglicht Einschränkungen, die darauf abzielen, dass der in einem Vertragsstaat geltende Datenschutz nicht durch den Grundsatz des freien transnationalen Informationsflusses zwischen Vertragsstaaten, z.B. durch eine Verlagerung von Verarbeitungshandlungen und Datenbanken, umgangen oder ausgehöhlt wird. So kann nach lit. a ein Vertragsstaat in Abweichung des Grundsatzes des freien Exportes spezielle Schutzmassnahmen ergreifen, wenn die Datenschutzbestimmungen eines andern Mitgliedstaates materiell verschieden sind oder, in Uebereinstimmung mit Art. 11, ein ausgedehnteres Schutzdispositiv aufstellen.⁶³ Wie erwähnt, können - durch die national unterschiedliche Ausgestaltung der Gesetze - mit Hilfe dieser Vorschrift neue Datenhindernisse entstehen, die nicht mehr nur auf einem unterschiedlichen Anwendungsbereich (Schutz juristischer Personen und (oder nur) natürlicher Personen, manuelle und (oder nur) automatische Verarbeitungsvorgänge etc.) beruhen, sondern auf einer abweichenden Regelungsdichte.

63 Vgl. Art. 11, vorne, gg), S. 256.

Lit. b unterbindet eine für ein Konventionsgebiet typische Erscheinungsform und Ausweichmöglichkeit: Den Datentransfer in einen Nicht-Mitgliedstaat über die Zwischenstufe eines andern Vertragsstaaten (ev. mit einer weniger restriktiven Gesetzgebung). Die Einschränkung nach lit. b ist aber nur anwendbar, wenn klar ersichtlich ist, dass die übermittelten Daten den Vertragsstaat wegen der erleichterten Ausfuhr in den Drittstaat passieren. Bei blosser Annahme oder in Erwartung, dass die Daten von einem Vertragsstaat in einen Drittstaat exportiert werden könnten, darf die Ausnahme nach lit. b nicht angewandt werden.

Mit dieser Formel wird eine Lösung des Problems der Ausfuhr von bereits innerhalb des Konventionsgebietes exportierten Daten an einen Nicht-Mitgliedstaat angestrebt. Die vorgeschlagene Regelung der Beschränkung des freien Datenflusses, falls ein anderer Vertragsstaat bloss als Transitterritorium für die Ausfuhr in einen Drittland dient, genügt m.E. für einen ausreichenden Schutz gegen die Umgehung der Bestimmungen des ersten exportierenden Vertragsstaates (Ursprungslandes) nicht. Die heutigen Mittel der EDV ermöglichen das Zwischen- oder Einschalten eines Verarbeitungsvorganges im exportfreundlichen Vertragsstaat, so dass dessen Territorium nicht mehr bloss passiert, sondern nach Durchführung eines spezifischen Datenverarbeitungsvorganges ⁶⁴ verlassen wird. Der dazwischengeschaltete Vertragsstaat ist dann kein "Transitstaat" nach der Bestimmung des lit. b mehr,

64 Ein möglicher Verarbeitungsvorgang ist z.B. das Sortieren von Daten: Im Ursprungsland, das den Export in den Drittstaat verbieten würde, wird die Verarbeitung soweit vorgenommen, dass im exportfreundlichen Vertragsstaat nur noch ein Sortiervorgang vorgenommen werden muss, obwohl er noch am gleichen Ort ausgeführt werden könnte. Das Charakteristische dieses Vorganges ist, dass der Datenbestand seinem Inhalt nach noch identisch ist und keine materielle Veränderung erfahren hat, sondern nur die Reihenfolge der Daten aufgrund des Sortiervorganges nach einem bestimmten Kriterium verändert wurde. Dies zeigt, dass ein Verarbeitungsvorgang erfolgt ist und somit nach lit. b kein blosses Passieren mehr vorliegt; de facto kann aber durch das Dazwischenschalten eines rein formellen Verarbeitungsschrittes, die Bestimmung umgangen werden: Somit existiert trotzdem eine legale Umgehungsmöglichkeit des Exportes in Drittländer nach der Bestimmung des lit. b.

bleibt aber de facto doch ein Transitland, weil keine Aenderung in der materiellen Substanz der Daten bzw. Datensätze erfolgt ist. Die Formulierung dieser Bestimmung müsste einen weiteren Tatbestand abdecken und z.B. das Verbot des Exportes über einen Vertragsstaat als Zwischenglied grundsätzlich untersagen, wenn damit die Umgehung der Vorschriften des Ursprungsstaates wirksam verhindert werden sollten; neben diesem Vorschlag existieren aber noch andere Lösungsmöglichkeiten.⁶⁵

Es ist in dem von der Konvention vorgesehenen Fall nicht vermeidbar, dass bei einem gleichzeitigen Export in Vertragsstaaten und Drittländer der Ursprungsstaat, der ein Genehmigungssystem gegenüber Drittstaaten kennt, dieses auch auf Konventionsstaaten anwendet, falls diese die Angaben anschliessend an ein Drittland weiterleiten, weil diese Genehmigung - vom Gesichtspunkt des Ursprungsstaates - auch den Export vom zwischengeschalteten Mitgliedsland direkt in den Drittstaat impliziert.

Die in der KE verwirklichte Lösung ist weder wirksam noch kompatibel, falls ein Staat sowohl die Konvention des Europarates ratifiziert als auch die Richtlinien der OECD unterzeichnet hat, weil letztere ihn auf eine liberale Haltung zu internationalen Datenflüssen verpflichten.

D. Mechanismen für gegenseitige Rechtshilfe zwischen Signatarstaaten

Das 4. Kapitel orientiert sich an den Konventionen über die Rechtshilfe in Verwaltungssachen und zeigt erneut die Uebertragung des öffentlich-rechtlichen Datenschutzmodells auf den privaten Bereich ohne eine differenzierte Normierung und Ausgestaltung dieser beiden Bereiche.

a) Allgemeine Zusammenarbeit

Die in der Konvention ausgearbeiteten Mechanismen sehen eine behördliche Zusammenarbeit zwischen den Mitgliedsstaaten vor, welche

65 Vgl. hinten, S. 324ff.

einerseits die Rechtshilfe bei der Durchsetzung der individuellen Ansprüche des Datensubjektes im Ausland gewährleisten und andererseits die Entwicklung der Konvention zu einem zwischenstaatlichen Regelwerk ⁶⁶ fördern soll. Auf die Schaffung einer internationalen Superbehörde wird verzichtet.

Diese Zusammenarbeit bedingt eine Bestimmung und genaue Bezeichnung der für die Rechtshilfe zuständigen Behörde; ^{67 68 69} die vorgesehene Zusammenarbeit ist weitreichend und beinhaltet sowohl präventive als auch nachgehende Kontrollen sowie Rechtshilfe und Erfüllung von Auskunftbegehren. Die Zulässigkeit solcher Begehren ist nach dem geltenden nationalen Recht zu beurteilen, so dass eine Behörde nicht über alle Datensammlungen Auskunft erteilen muss und darf (gemäss Legalitätsprinzip), sondern unter Hinweis auf den "ordre public" Verweigerungsgründe geltend machen kann. ⁷⁰ Die Rechtshilfebegehren von Behörden ⁷¹ sollten aber grundsätzlich nur zur Verwirklichung der Datenschutzprinzipien der Konvention gestellt werden.

Hier fragt sich, ob man für die Rechtshilfebegehren von Behörden nicht ebenfalls eine genaue Angabe des Grundes und Zweckes verlangen sollte, wie für die Durchsetzung privater Ansprüche? ⁷²

b) Rechtshilfe für ausländische Datensubjekte ⁷³

Da die Konvention keine speziellen Bestimmungen über das auf einen internationalen Tatbestand anwendbare Recht enthält, ⁷⁴ wird

66 Vgl. auch 5. Kapitel zum Konsultativkomitee.

67 I.d.R. wird es die Datenschutzbehörde eines Landes sein.

68 Bei mehreren Behörden (z.B. im föderalistischen System) muss der Kompetenzbereich einer jeden Behörde festgesetzt werden, was im Interesse der Rechtshilfe suchenden ausländischen Stellen nicht sehr zweckmässig erscheint (gl.M. AUERNAHMMER, DS+DS 4/80, S. 182).

69 Die Konvention verlangt nicht, dass jeder Staat eine (Datenschutz-) Behörde hat, es muss nur eine solche für die Zusammenarbeit und die Zwecke der Konvention bezeichnet werden.

70 Damit soll verhindert werden, dass Staaten bzw. Behörden einander gegenseitig den Inhalt von Datenbanken preisgeben.

71 Art. 14 Abs. 3 lit. a und b (Rechtshilfe von Behörden).

72 Vgl. nachfolgend c), S. 263 und Art. 14 Abs. 3 lit. a - c.

73 Art. 14 KE.

74 Vgl. hinten. S. 267ff.

über die Rechtshilfe ein Forum für die Geltendmachung der Ansprüche von Ausländern geschaffen. Dabei kann im Einzelfalle fraglich sein, ob ein Vertragsstaat einem Ausländer aufgrund seines internen Datenschutzrechts überhaupt Rechtshilfe zur Geltendmachung seiner Ansprüche gemäss Art. 8 anbieten kann.⁷⁵ Die Konvention enthält keine befriedigende Aussage, wie dem Betroffenen eine Rechtshilfe für die Durchsetzung seiner Individualrechte in einem komplexen, sich über mehrere Staaten erstreckenden Informationssystem geleistet wird.

Das Wahlrecht des Datensubjektes, das in einem Vertragsstaat wohnt, sein Individualrecht direkt im Land der Verarbeitung oder indirekt über die Behörde des Auslandes oder über die diplomatische Vertretung seines Heimatlandes als Vermittler geltend zu machen, ist positiv, dürfte aber in der Praxis den grössten Teil der Betroffenen überfordern, sei es wegen der Schwierigkeit der geographischen Ortung eines Verarbeitungsvorganges in einem integrierten Datennetz, sei es wegen der Sprachprobleme oder wegen der erschwerten Bestimmbarkeit der zuständigen Behörde innerhalb eines föderalistisch strukturierten Staates.

c) Spezifikation des Rechtshilfebegehrens⁷⁶

Jedes Rechtshilfebegehren durch einen Privaten unterliegt der detaillierten Angabe des Grundes und Zweckes des Begehrens sowie der Bezeichnung des Petenten und der Bestimmung der Daten bzw. Datenbank. Negativ erscheint mir, dass diese Spezifikation der Gründe einzig von privaten Geschuestellern verlangt wird und nicht auch für öffentliche Stellen⁷⁷ vorgesehen ist.

d) Schutzmassnahmen zur Rechtshilfe⁷⁸

Hier stellt sich die Frage, ob die vorgesehenen Schutzmassnahmen ausreichen, um andere Verwendungsmöglichkeiten der erhaltenen Informationen durch eine Behörde, die um Auskunft ersucht, zu vermeiden.

75 Z.B. bei blossen Zugriff über einen Terminal im Inland auf eine Datenbank im Ausland.

76 Art. 14 Abs. 3 KE.

77 Vgl. vorgehend a), S. 262.

Es wird zwar statuiert, dass die ersuchende Behörde, die aufgrund von Rechtshilfebegehren Informationen erhalten hat, diese nur für den spezifizierten Zweck verwenden darf und deren Vertraulichkeit wahren muss, doch wird nirgends explizit verlangt, dass die gesuchstellende Behörde Grund und Zweck des Begehrens näher bezeichnen muss. Da eine ausdrückliche Zweckfestsetzung nicht erfolgt, ist deren zweckgemässe Verwendung nur schwer zu beurteilen.

Bei der Beachtung des Geheimhaltungsprinzips könnten beim föderalistischen System Schwierigkeiten auftreten, wenn die Bundesbehörde Informationen an eine Landesbehörde weiterleiten möchte.

Das Verbot der behördlichen Selbstermächtigung zu Nachforschungen mittels Rechtshilfebegehren durch eine Behörde ohne spezielle Einwilligung des Datensubjektes, in dessen Namen das Gesuch gestellt wird, ist verständlich und bildet Voraussetzung gegenseitigen Vertrauens, auf dem die Rechtshilfe basiert.

e) Abweisung eines Rechtshilfebegehrens ⁷⁹

Die grundsätzliche Verpflichtung zur Erfüllung des Rechtshilfebegehrens und die abschliessende Aufzählung der Verweigerungsgründe vermögen eine wegen der unterschiedlich weitgehenden Einsichts- und Kontrollrechte der nationalen Behörden entstehende Unausgewogenheit zwischen den Vertragsstaaten nicht auszuschalten. So könnte es z.B. für einen temporär in Schweden wohnhaften Ausländer nachteilig sein, wenn sein Heimatstaat mittels eines Rechtshilfegesuches infolge der sehr weitgehenden Kognitionsbefugnis der schwedischen Datenschutzbehörde umfangreichere Informationen erhält, als er über die Datensubjekte des eigenen Landes erfahren könnte.

Hier könnte die Anwendung des Grundsatzes der Reziprozität einen Ausgleich schaffen, indem Auskunfts- und Rechtshilfeansprüche der gesuchstellenden Behörde nur in dem Umfang ausgeführt werden, als sie für die ersuchende Behörde nach der einheimischen Rechtsordnung zugelassen sind.

78 Art. 15 KE.

79 Art. 16 KE.

f) Kosten und Verfahren der Rechtshilfe⁸⁰

Die Behandlung von Rechtshilfebegehren von in- und ausländischen Betroffenen sowie das Verbot einer speziellen diskriminierenden Kostenbelastung von ausländischen Datensubjekten dient der Verwirklichung des Persönlichkeitsschutzes auf internationaler Ebene. Allerdings dürften die Kosten für Datenverarbeitungs-Experten, die Testläufe und Ueberprüfungen der Sicherungsmassnahmen eines DV-Systems vornehmen, eine erhebliche Belastung darstellen und das Datensubjekt von der Geltendmachung seiner Rechte in einem Streitfalle, der nur mit Hilfe eines Experten gelöst werden kann, abhalten. Hier könnte die Kostenverteilung u.U. einen Weg eröffnen, der die Durchsetzung von Persönlichkeitsverletzungen indirekt zu verhindern vermöchte. Eine Lösung könnte darin gefunden werden, dass die Expertenkosten bei einem negativen Entscheid des Experten auf den Wohnsitzstaat des gesuchstellenden Datensubjektes überwältzt, bei positivem Entscheid aber, d.h. bei Mängeln im Sicherungssystem, die Kosten der verantwortlichen Stelle auferlegt werden. M.E. würde dies ausserdem eine Vorprüfung des privaten Gesuches durch den ersuchenden Staat voraussetzen, damit er nicht Kosten für leichtfertige Begehren übernehmen muss.

Für die Uebersetzungskosten wäre die Abwälzung der Kostenlast auf den Staat der ersuchenden Behörde sachgerecht, v.a. im europäischen und internationalen Raum mit seiner Sprachvielfalt.

Die Möglichkeit spezieller zwischenstaatlicher Vereinbarungen über Verfahrensfragen, Form und Sprache etc. vermag zwar die unterschiedliche Behandlung des öffentlichen und privaten Sektors, ebenso wie die spezieller Datenkategorien, zu berücksichtigen, sollte aber nicht dazu genutzt werden, bilaterale Vereinbarungen über die Anwendbarkeit des Rechts, der örtlichen, sachlichen und funktionellen Zuständigkeit abzuschliessen, weil entsprechende Vorschriften in der Konvention fehlen.

80 Art. 17 KE.

g) Konsultativ - Komitee ⁸¹

Die Schaffung eines Konsultativ-Komitees oder beratenden Ausschusses bildet eine geglückte Ergänzung des Rechtshilfesystems. Seine Funktion ist beratender und konsultativer Natur und soll eine reibungslose Anwendung, die Entwicklung von Verbesserungen sowie eine Lösung von Fragen der praktischen Einführung der Konvention gewährleisten. Durch den Verzicht, dieses Komitee als Entscheidungsbehörde bei Streitigkeiten einzusetzen, wurde bewusst dem Konzept einer internationalen "Super-Datenschutzbehörde" eine Absage erteilt.

E) Territorialklausel ⁸²

Die Ausdehnung des Anwendungsgebietes auf entfernte Territorien eines Vertragsstaates bei der Ratifikation kann eine ambivalente Wirkung erzielen.

Positiv wirkt sie sich sicher auf die datenverarbeitenden Stellen eines Landes mit überseeischen Territorien, wenn mittels der DV Zeitverschiebung und die Vorteile von Niedrig-Lohn-Länder ausgenutzt werden sollen und die Daten dabei innerhalb des gleichen gesetzlichen Geltungsbereiches verbleiben. Diese meist auf der Stufe von Entwicklungsländer befindlichen Territorien erhalten ausserdem eine Aufwertung durch den Import des technischen "know-hows" und der Förderung des technologischen Ausbaus, was letztlich in einer stufenweisen Integration solcher Gebiete in die Vereinigung der datenschutzbewussten Nationen gleichkommt.

Negativ kann sich eventuell ein mangelndes Schutzbewusstsein dieser Gebiete, die zivilisatorisch noch nicht die Stufe der westlichen Industrieländer erreicht haben, auswirken und einem Konventionsgebiet dadurch potentielle "data havens" drohen.

81 Art. 18 - 20, vgl. auch Art. 21 KE.

82 Art. 24 KE.

3. Folgerung

Das in der Präambel in Form von Postulaten ⁸³ gesteckte Ziel der Konvention ist mit den niedergelegten Bestimmungen m.E. nicht erreicht worden. Diese Ziele sind mittels der gewählten Form und rechtlichen Ordnung nicht realisierbar, vor allem wegen des nicht zwingenden Charakters der Konvention und der zahlreichen Einschränkungs- und Ausdehnungsmöglichkeiten.

Die Einigung auf einen Minimalstandard an Datenschutz - in Form des *noyau dur* - mit den verschiedenen Sollbruchstellen genügt alleine nicht, um die schwierigen Probleme der Bestimmung des zuständigen Forums und des anwendbaren Rechts befriedigend zu lösen. Der Begleitbericht erwähnt, ⁸⁴ dass das Expertenkomitee bewusst darauf verzichtete, eine definitive Regelung zu diesem Thema in die Konvention aufzunehmen. ⁸⁵ Das Vorhandensein des *noyau dur* mit materiellem Recht, welcher teilweise aber auch Verfahren harmonisieren soll, ist nach Meinung des Expertenkomitees dazu angetan, das Risiko von Gesetzeskonflikten oder Gesetzeslücken zu vermindern. ⁸⁶ Diese Feststellung ist grundsätzlich richtig, stellt aber keine befriedigende Lösung dar, solange die Gefahr von Gesetzeskonflikten, Gesetzeslücken und Zuständigkeitsproblemen zwischen Vertragsstaaten nicht vollständig gebannt und das Problem abschliessend gelöst ist. Gesetzeskollisionen entstehen aber nicht nur aus dem Verhältnis der Mitgliedstaaten untereinander, sondern auch zwischen dem Konventionsgebiet und Drittstaaten, die mit einem Konventionsland den grenzüberschreitenden Datenverkehr pflegen. Eine Lösung dieser anstehenden, wichtigen Fragen ist mit Hilfe des *noyau dur* aber nicht erreichbar.

Das in der Konvention zum grenzüberschreitenden Datenverkehr vorgesehene Kapitel und die übrigen Teile vermögen keine befriedigende

83 Vgl. vorne, S. 242f.

84 CONSEIL DE L' EUROPE, Rapport explicatif, N 23.

85 Es ist allerdings fraglich, ob ein für spätere Zeit beabsichtigter, ergänzender Zusatz in Form eines Protokolls (id., a.a.O., N 23) angesichts des "non self executing"-Charakters geeignet ist, die anstehenden Fragen zufriedenstellend zu lösen.

86 CONSEIL DE L' EUROPE, a.a.O., N 23.

Regelung der internationalen Datenflüsse zu geben. Für deren Lösung könnten materielle Bestimmungen einen realisierbaren Ansatz darstellen: Sie müssten eine Aussage enthalten,

- welches Recht bei Verarbeitungsvorgängen, die sich auf mehrere Vertragsstaaten erstrecken, auf den einzelnen Vorgang bzw. gesamten Verarbeitungsprozess zur Anwendung kommen soll und zwar einerseits zwischen Vertragsstaaten, andererseits zwischen Konventionsländern und Drittstaaten.⁸⁷
- wie das Prinzip der Transparenz bei internationalen Datenflüssen realisiert werden soll, z.B. Zulässigkeitsvoraussetzungen einer Weitergabe im internationalen Bereich.
- über den Standard von Datenschutzmassnahmen im internationalen Datenverkehr, d.h. differenzierte Anforderungen⁸⁸ je nach Uebertragungsart (packet-switching, circuit-switching, Satellit, etc.)
- zur Verwirklichung des freien Datenflusses durch ein Verbot spezieller Genehmigungen gegenüber Mitgliedstaaten, nicht nur hinsichtlich des Exportes, sondern auch des Importes.
- dass Import bzw. Reimport von Daten nicht zur Ausnützung und Umgehung der Gesetzesregelung des Exportstaates missbraucht werden dürfen.
- wie die bereits im Zusammenhang mit Anträgen des Datensubjektes bzw. einer Behörde gestellten Rechtshilfen auf die Untersuchungsphase wie auch auf die Vollstreckungsphase⁸⁹ ausgedehnt werden können.
- wie die Weiterleitung von Urteilen, Verfügungen und Massnahmen, die im Zusammenhang mit einem gesetzeswidrigen Datenverarbeitungsvorgang in einem Vertragsstaat erfolgt sind, welcher grenzüber-

87 Vgl. auch die von GOTLIEB/DALFEN/KATZ (S. 251) vorgeschlagene "residual application of laws": i.e. z.B., dass US-Kreditbüros in Kanada den Fair Credit Reporting Act anwenden, wenn im kanadischen Gesetzesraum noch kein solches Gesetz vorhanden ist.

88 Bei Satellitenkommunikation z.B. Pflicht zur HW- und/oder SW-mässigen Verschlüsselung.

89 Z.B. Löschung von Datenbanken im Ausland.

schreitenden Charakter hat, auch an die andern interessierten Signatarländer erfolgen soll.

- wo überall die Individualrechte und Ansprüche geltend gemacht werden können, z.B. an einem bestimmten Forum, dessen Recht auch zur Lösung des internationalen Tatbestandes zuständig ist⁹⁰ oder an mehreren Orten, d.h. dort wo eine Verarbeitungshandlung durchgeführt wurde,⁹¹ mit entsprechender Weiterleitungspflicht der mit einem Rechtsbehelf angegangenen Behörden eines Vertragsstaates an die Behörden des zuständigen anderen Mitgliedslandes.
- über gesetzliche Bestimmungen zum Datenverkehr von Vertragsstaaten mit internationalen Organisationen⁹² und gegebenenfalls über den Datenverkehr innerhalb von multinationalen Gesellschaften, deren Niederlassungen sowohl in Vertragsstaaten als auch in Drittländern, mit und ohne Datenschutzgesetzgebung, angesiedelt sind.
- wie wirksam verhindert wird, dass Daten, die innerhalb des Konventionsgebietes bereits exportiert wurden, nicht über einen Vertragsstaat mit largier Gesetzgebung an einen Drittstaat gelangen, auch wenn sie im ersteren einem Verarbeitungsvorgang unterworfen werden.

Der Ausgleich von Informationsfreiheit und Datenschutz wird durch die Beschränkung des Schutzbereiches auf natürliche Personen von der Konvention selbst verunmöglicht: Diese Begrenzung lässt nicht nur ein gestecktes Ziel offen, sondern verhindert ausserdem eine Befriedigung des Bedürfnisses nach einem Interessenausgleich im Bereich der Wirtschaft, in dem der Hauptanteil des transnationalen Informationsumschlages stattfindet.

Die formalrechtliche Ausgestaltung des Entwurfes als "non self-executing Convention" ist m.E. wenig geeignet, die anstehenden Fragen des Datenschutzrechts auf internationaler Ebene befriedigend zu lösen.

89 Einheit von "Jus und Forum", vgl. hinten, S. 305f.

91 Ubiquitätsprinzip bedeutet zugleich ein Auseinanderfallen von Jus und Forum.

92 Soweit diese nicht einen extraterritorialen Status geniessen.

Zahlreiche Problemkreise⁹³ des Datenschutzrechts sind durch bloße Aufnahme einer vereinheitlichten Norm in der nationalen Gesetzgebung nicht zufriedenstellend lösbar, sondern bedürfen aufgrund der international gleichgelagerten Problemstellung einer rechtsetzenden materiellen Norm auf supranationaler Ebene: Z.B. mittels eines internationalen Rechtsregimes, dessen Bestimmungen für die Signatarländer einen imperativen Charakter haben, i.d.S., dass aus ihnen Rechte herleitbar sind. So kann auf spezifische Anforderungen⁹⁴ mit einem wirksamen Persönlichkeitsschutz geantwortet werden und verursachen, dass ein effektiver Schutzraum gegenüber Drittstaaten entsteht, dessen Wirkung auf die letzteren repressiver Natur ist und sie einem gewissen Beitrittszwang aussetzt. M.E. ist mit einer internationalen Konvention ohne einen Kern von Einheitsrecht bildenden Bestimmungen kein effektiver Schutzraum zu realisieren. Ein von Sollbruchstellen durchlöcher-tes Schutzgebiet wirkt aber auf Drittstaaten nicht anziehend, sondern ermutigt sie, der Konvention fernzubleiben, weil die konventionsinter-nen Ungleichheiten den Bewegungsfreiraum mehr einschränken als Vorteile für den freien grenzüberschreitenden Datenfluss bringen, so dass letztlich die mit dem internationalen Datenverkehr beschäftigten Per-sonen in Drittstaaten besser gestellt sind, als in Vertragsstaaten. Dies ist aber nicht Sinn und Ziel einer völkerrechtlichen Konvention.

Der Europarat sollte also versuchen, neben jenen Gesetzgebungs-grundsätzen des noyau dur, welche primär die nationale Datenschutzge-setzgebung betreffen und dadurch nur indirekt, aufgrund des angestreb-ten gleichmässigen Niveaus nationaler Datenschutzrechte, zum Daten-schutz im transnationalen Informationsverkehr beitragen, eine Anzahl von Grundsätzen materieller Natur zu entwickeln, welche spezifische Fragen des grenzüberschreitenden Datenverkehrs zum Gegenstand haben.

93 Vgl. Aufzählung vorne, S. 268f.

94 Ein klares einheitliches Konzept im Vertragsgebiet zur Ausfuhr von bereits übermittelten Daten an Drittstaaten kann neue Daten-hindernisse ("Convention havens") vermeiden helfen, z.B. solche, die sich aus dem Datentransfer via Satellitenübertragung erge-ben.

III. OECD: Richtlinien zum Datenschutz ⁹⁵

1. Vorbemerkung

Gegenstand der nachfolgenden Ausführungen bilden die vom Ministerrat der OECD am 23. September 1980 als Beilage zu einer Empfehlung verabschiedeten Richtlinien für den Schutz der Privatsphäre und die grenzüberschreitende Uebermittlung personenbezogener Daten.

"Diese Leitlinien weisen erhebliche inhaltliche Aehnlichkeiten mit der Datenschutzkonvention des Europarates auf"⁹⁶: Ich beschränke meine Erläuterungen deshalb auf die Grundzüge der RL und die signifikantesten Abweichungen bzw. Unterschiede gegenüber der KE. Ein detaillierter Kommentar zu den RL ist im "Explanatory Memorandum"⁹⁷ zu finden.

2. Form der Richtlinien

Bei den RL handelt es sich um Empfehlungen der OECD zur Harmonisierung der Datenschutzvorschriften an die Adresse ihrer Mitgliedstaaten, die rechtlich nicht bindenden Charakter haben und weder einen Beitritt noch eine Ratifikation durch die OECD-Mitgliedstaaten erfordern. Es handelt sich hier um eine juristische Konstruktion i.S. von Verhaltensregeln zu deren Einhaltung aber keine rechtliche Verpflichtung besteht; ein Einzelner kann aus ihnen auch keine Rechte und Ansprüche ableiten.

Im Gegensatz dazu ist die Konvention des Europarates für diejenigen Mitgliedstaaten bindend, welche sie ratifiziert haben. Da ihre Konzeption auf der "non self executing power" beruht, müssen die Vorschriften der Konvention in nationales Recht übergeführt werden, da aus ihr selbst keine Rechte hergeleitet werden können.

3. Inhalt der Richtlinien

Die Gliederung und der Aufbau der RL gleicht sehr demjenigen der

95 "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Adopted by the Council at its 523rd Meeting on 23rd September, 1980, in: Dok. Nr.: OECD, C (80) 58 (Final).

96 AUERNHAMMER, DS+DS 4/80, S 182.

97 OECD, Dok. Nr.: C (80) 58 (Final).

KE: Bei der Ausarbeitung dieser "Guidelines" und der Konvention wurde auch darauf geachtet, dass keine unnötigen textlichen Differenzen zwischen den beiden Abkommen entstanden. Das Herz der RL bilden ebenso wie bei der KE die Basisprinzipien zum Schutz von Privatsphäre und Grundfreiheiten auf nationaler Ebene⁹⁸. Das Problem der Vermeidung von "data havens" wird im Bereich der internationalen Datenflüsse aufgegriffen. Es erfolgt keine Unterscheidung zwischen Export und Import bzw. Reexport und Reimport, da alle Vorgänge die Rechte von Personen gleichermaßen zu beeinträchtigen vermögen.

A. Teil I. und Präambel

a) Präambel

Die Präambel ist nicht von der gleichen Philosophie inspiriert wie die der KE. So bemühen sich zwar beide um einen Ausgleich der gegensätzlichen Interessen aus Datenschutz und Informationsfreiheit sowie um die Wahrung der Privatsphäre im grenzüberschreitenden Datenverkehr, hingegen wird bei den RL zusätzlich noch die Bedeutung der transnationalen Datenflüsse auf die Beziehungen der Staaten zueinander und deren Beitrag zur wirtschaftlichen und sozialen Entwicklung betont.

Im Gegensatz zur KE bleibt aber bei den RL das Problem des Ausgleichs des Spannungsverhältnisses von Datenschutz und freiem Informationsfluss nicht unbeantwortet, sondern nimmt neben den Grundsätzen zum Datenschutz im III. Teil eine bedeutende Stellung ein.⁹⁹

b) Teil I.

Aufgrund der unterschiedlichen formalen Konzeption der RL ist ihr Detaillierungsgrad viel geringer als derjenige der KE. Die Definitionen (§ 1 RL) decken sich weitgehend mit demjenigen der KE. Erwähnenswert ist, dass die RL unter dem Begriff des grenzüberschreitenden Datenverkehrs auch die Datenübertragung via Satelliten verstehen.¹⁰⁰

98 Noyau dur.

99 vgl. hinten, S. 277ff.

100 OECD, Explanatory Memorandum, N 42.

aa) Anwendungsbereich

Der Anwendungsbereich beschränkt sich ebenfalls nur auf den Schutz personenbezogener Daten natürlicher Personen (§ 2 i.V. mit § 1 lit. b RL), da das Expertenkomitee keinen Konsens über den Einbezug der juristischen Personen, Vereinigungen und Personengruppen in den Schutzbereich erzielen konnte. Es bleibt somit den einzelnen Mitgliedstaaten überlassen, die Trennungslinien gegenüber juristischen Personen, Personengruppen oder andern rechtlichen Gebilden zu ziehen bzw. den Schutz auszudehnen.¹⁰¹ Die damit verbundenen Nachteile müssen nicht nochmals in ihrer Gesamtheit erwähnt werden.¹⁰²

Im Gegensatz zur KE fallen sowohl automatisiert als auch manuell verarbeitete Daten in den Geltungsbereich (§ 2 RL). Hier wurde erkannt, dass es schwierig ist, im Hinblick auf die Schutzentfaltung eine klare Trennung zwischen manuell und automatisiert verarbeiteten Daten durchzuführen; ausserdem wollte man die Entstehung von Unvereinbarkeiten und Lücken vermeiden und die Möglichkeit der Gesetzesumgehung über manuelle Mittel unterbinden.¹⁰³ Diese Ueberlegungen sind beherrscht von der Ueberzeugung, dass die Prinzipien des Persönlichkeitsschutzes nicht von der Technologie abhängen - sie vermochte nur die Datenschutz-Diskussion zu aktualisieren -, sondern von der Verarbeitung der personenbezogenen Daten schlechthin. Dieser generelle Schutz kann aber bei einer Beschränkung auf die automatischen Verarbeitungsvorgänge durchbrochen werden.

Die Abgrenzung gegenüber den zu persönlichen Zwecken manuell verarbeiteten Daten bzw. Datensammlungen (wie z.B. persönliche Notizbücher) richtet sich nach dem offensichtlich nicht potentiell schädlichen Charakter dieser Art von Datensammlungen.

Der Geltungsbereich erstreckt sich auf den privaten wie auf den öffentlichen Sektor, kann aber von den Mitgliedstaaten abweichend festgelegt werden.

Die Richtlinien sehen auch Abweichungsmöglichkeiten der Schutzmassnahmen in graduell unterschiedlichen Sensitivitätsstufen von

101 Id., a.a.O., N 33.

102 Vgl. vorne KE, S. 244ff.

103 Vgl. OECD, Explanatory Memorandum, N 34, 35.

Daten vor und zwar hinsichtlich ihres Kontextes und in Relation zu deren Verarbeitungsvorgängen. So ist grundsätzlich auch der Ausschluss trivialer Daten vom Anwendungsbereich möglich (§ 3 RL).

bb) Ausnahmen

Obwohl Ausnahmen in einer nicht bindenden Empfehlung überflüssig erscheinen, werden die zu den Prinzipien der Teile II. und III. möglichen Ausnahmen beschränkt und bestimmten Grundsätzen unterworfen. Damit wird verhindert, dass die Prinzipien zum Minimalstandard und zur Regulierung des grenzüberschreitenden Datenverkehrs durch Souveränitäts-, nationale Sicherheitsinteressen oder den "ordre public" durchlöchert und der Mindestschutz weiter reduziert wird (§ 4 RL). Bemerkenswert ist die Anwendung dieser Grundsätze auf die Ausnahmeregelungen, die die Mitgliedsstaaten anhalten, so wenig wie möglich Ausnahmen von den Grundprinzipien der Teile II. und III. vorzusehen und, falls solche unumgänglich sind, dafür zu sorgen, dass diese der Allgemeinheit auch bekannt sind.

Für föderalistisch strukturierte Staaten wird betont, dass zur Anwendung der Richtlinien kein Durchbrechen der verfassungsmässigen Schranken notwendig ist, sondern ein Vorschlag erteilt, wie die Anwendung der "Guidelines" auch unterhalb der Stufe des Bundesrechts verwirklicht werden kann (§ 5 RL).

Die Richtlinien werden ausdrücklich als Minimalstandard betrachtet, so dass einem weitergehenden Schutz durch spezielle nationale Vorschriften kein Hindernis entgegensteht (§ 6 RL).

B. Teil II.

a) Ziel und Zweck

Teil II. (§§ 7 - 14 RL) bildet wie der noyau der KE den Kern der Richtlinien und besteht aus Grundprinzipien zum Datenschutz, die sich sowohl gegenseitig bedingen als auch teilweise überlappen. Gegenstand dieser Prinzipien ist die Qualität der Daten, die Festsetzung des Zweckes der Datenverarbeitung, die Festlegung der Schranken hinsichtlich ihrer Verwendungsmöglichkeiten, die Pflicht zur Datensicherung sowie die Verankerung von Individualrechten (Einsichtsrecht, Auskunftsrecht, Berichtigungsrecht).

Zweck und Ziel der Prinzipien decken sich praktisch mit denjenigen der Europarats-Konvention und bestehen darin,¹⁰⁴

- mit Hilfe der Zustimmung der Mitgliedsstaaten ein Mindestmass an Datenschutz aufzubauen und die individuellen Freiheitsrechte zu garantieren.
- die Differenzen zwischen den grundlegenden nationalen Regeln und Praktiken unter den Mitgliedsstaaten auf ein Minimum zu reduzieren.
- sicherzustellen, dass die Mitglieder beim Schutz personenbezogener Daten auch die Interessen anderer Mitgliedsländer berücksichtigen und das Bedürfnis und die Vorteile eines ungehinderten Datenflusses erkennen.
- die Ursachen zu beseitigen, die einzelne Mitglieder veranlassen könnte, den grenzüberschreitenden Datenverkehr gegenseitig zu reduzieren und zu beschränken.

Die Prinzipien sind somit ein Teil zur Verwirklichung der Zielprojektion der "Guidelines" schlechthin: des Ausgleichs der Interessen am Schutz der Privatsphäre und der individuellen Freiheit (z.B. als informationelles Selbstbestimmungsrecht) einerseits und am ungehinderten, grenzüberschreitenden Verkehr personenbezogener Daten i.S. eines freien Informationsflusses andererseits.

b) Inhalt der einzelnen Prinzipien

Inhaltlich decken sie sich ebenfalls mit denjenigen der KE,¹⁰⁵ wobei einige materiellrechtliche Abweichungen auftreten, z.B. bedingt durch den auf manuell verarbeitete Daten erweiterten Anwendungsbereich:

So existiert im Gegensatz zur KE¹⁰⁶ auch ein Prinzip hinsichtlich der Begrenzung des Sammelns von Daten (§ 7 RL), das eine Festsetzung von Schranken nach verschiedenen Kriterien befürwortet: Z.B.

- Schranken, die sich aufgrund der Natur des Kontextes der Daten ergeben oder

¹⁰⁴ Vgl. id., a.a.O., N 25.

¹⁰⁵ Vgl. vorne, S. 250ff.

¹⁰⁶ Ist in der KE nur im Zusammenhang mit dem grenzüberschreitenden Datenverkehr dem Anwendungsbereich unterstellt, hingegen nicht als Grundprinzip des *noyau dur*.

- Schranken, die aus der speziellen Zweckverwendung einer Verarbeitung bzw. ihrer Verarbeitungsvorgänge und deren nachfolgenden Benutzung resultieren, ferner
- verfassungsmässige und durch die übrige Rechtsordnung (wie z.B. Sittlichkeit) bedingte Schranken.

Neben diesen Kriterien wird das Postulat nach rechtskonformen und loyalen Sammelmethode als Bestandteil der Gesamtheit der Verarbeitungsschritte verankert.

Die RL machen keinen Unterschied in der Behandlung der Daten des öffentlichen und privaten Bereichs hinsichtlich ihrer Qualität (§ 8 RL), was u.U. nachteilige Auswirkungen vor allem im privaten Bereich haben könnte - allerdings muss hier beachtet werden, dass die RL keinen bindenden Charakter haben wie die KE. Auch hinsichtlich der Bestimmung des Zweckes der DV (§ 9 RL) wäre eine differenzierte Behandlung der beiden Bereiche empfehlenswert, vor allem deshalb, weil die Bekanntgabe dieser Zweckbestimmung bereichsspezifischer Formen bedarf: Im öffentlichen Bereich ist die Zweckbestimmung durch die gesetzliche Grundlage der DV gegeben und i.d.R. für jedermann erkennbar oder zumindest eruierbar, im privaten Sektor hingegen bedarf es anderer Methoden der Veröffentlichung.

In den RL wird auch das Prinzip der Transparenz der Datenverarbeitung (§ 12 RL) festgehalten, das als Vorbedingung zur Wahrnehmung der Individualrechte dient. Hier sollte m.E. ebenfalls eine Trennung zwischen öffentlichem und privatem Bereich erfolgen, da die öffentliche Zugänglichkeit sämtlicher Daten mit den grundlegenden Datenschutzprinzipien nicht unbedingt vereinbar ist. Hier muss in den nationalen Rechten, unter Berücksichtigung des Informationsmediums eine bereichsspezifische Lösung gefunden werden.

Die mit der Ausübung der Individualkontrolle (§ 13 RL) verbundenen Detailangaben, die die Individualrechte umrahmen (Frist, Gebühr und verständliche Form der Auskunftserteilung etc.) sind zu unbestimmt und müssten noch mehr konkretisiert werden. Eine höhere Detaillierungsstufe bei der Gebührenfrage sowie zum Zeitrahmen der Auskunftserteilung wäre sicherlich im Sinne der Festsetzung eines Höchstmasses vertretbar, zumal es sich um rein formelle Angelegenheiten handelt, deren Beitrag zur Verwirklichung eines Minimalniveaus an

Datenschutz jedoch nicht unterschätzt werden darf. Keine befriedigende Lösung vermittelt die dehnbare Fassung der "verständlichen Form der Auskunftserteilung", vor allem deshalb, weil sie eine wesentliche Voraussetzung für die Ausübung der Individualrechte darstellt. Da gerade im geographischen Bereich der OECD-Länder zahlreiche Sprachprobleme auftauchen können, ist eine detailliertere Verständigung auf bestimmte Grundregeln sicherlich von gegenseitigem Nutzen und Vorteil.

Im Verantwortlichkeitsprinzip der RL (§ 14) werden Funktion und Aufgaben der verantwortlichen Stelle eindeutig im Gesamtrahmen festgelegt und ihr damit bestimmte Verpflichtungen (zivil- und evtl. strafrechtliche Haftung) überbunden.

C. Teil III.: Prinzipien auf internationaler Ebene (§§ 15 - 18 RL)

Interessant im Vergleich zur KE sind die für den internationalen Bereich anwendbaren Prinzipien der RL. Während die KE durch die Beschränkung auf die Gewährleistung des freien Exportes bzw. Wiederausports ohne gleichzeitige Verpflichtung zu einem genehmigungsfreien Import bzw. Reimport den freien grenzüberschreitenden Datenverkehr nicht zu realisieren vermochte,¹⁰⁷ vermeiden die RL eine einseitige Betonung des Exportes bzw. des Importes, sondern postulieren immer nur einen freien Datenfluss. Damit werden sie dem in der Präambel gesteckten Ziel nach einem freien transnationalen Datenfluss gerecht.

Im Gegensatz zur KE enthalten die Prinzipien auch eine Aussage zur Realisierung des Ausgleiches der Interessen an Datenschutz und Informationsfreiheit als Ausdruck des freien Datenflusses.¹⁰⁸

In ihrem Inhalt kommt die Forderung nach nationalstaatlichen Massnahmen zur Sicherstellung des freien transnationalen Verkehrs personenbezogener Daten unter den Mitgliedstaaten deutlich zum Ausdruck,¹⁰⁹ sei es durch eine allgemeine Vorschrift oder durch spezielle Anleitungen zur Gestaltung des grenzüberschreitenden Datenver-

107 Vgl. vorne, S. 258ff.

108 Vgl. auch OECD, Explanatory Memorandum, N 25.

109 Die Betonung des freien, sicheren und ungehinderten Flusses ist z.B. aus der Forderung nach freiem Transit der Daten durch Mitgliedstaaten ersichtlich (§ 16 RL).

kehrs im nationalen Datenschutzrecht. Ausserdem werden die Mitgliedstaaten ausdrücklich angehalten, Erlasse, Gesetze, Verfahren und sonstige politische Massnahmen zu unterlassen, die für den Schutz der Persönlichkeitsrechte unverhältnismässig erscheinen und den freien Informationsfluss künstlich behindern (§ 18 RL).¹¹⁰

Dabei wird im besondern auf die negativen Auswirkungen verwiesen (d.h. die Entstehung neuer Schranken), die eine Nichtbefolgung der Grundprinzipien des Teiles II. durch einen Mitgliedstaat auf den freien Datenfluss hat. Es wird aber nicht nur zur Vermeidung von Gesetzesumgehungen durch Beachtung der materiellen Datenschutz-Bestimmungen im internen Verhältnis, d.h. unter den Mitgliedsstaaten, aufgefordert, sondern auch im externen Verhältnis, d.h. von Mitgliedstaaten gegenüber Drittstaaten, m.a.W. die Mitglieder sind verpflichtet, sicherzustellen, dass die personenbezogenen Angaben durch einen direkten Export oder über Transitwege nicht in Gebiete gelangen, die kein Datenschutzbewusstsein oder ein nur marginales Schutzsystem entwickelt haben. Denjenigen Staaten,¹¹¹ die den Schutz personenbezogener Daten auf Staatsbürger oder Ausländer mit Wohnsitzgenehmigung beschränken, wird die Aufnahme spezieller Normen empfohlen, die den Schutzbereich auch auf Daten von Ausländern ausdehnen und damit die Entstehung eines Freiraums für die Verarbeitung von Informationen über Datensubjekte verhindern, die nicht in die geschützten Kategorien fallen.¹¹² Eine solche Ungleichbehandlung würde zweifelsohne zur Entstehung eines "data havens" und zur Reaktion der übrigen Mitgliedsstaaten führen und ausserdem der Zielprojektion der Guidelines klar zuwiderlaufen.

So werden denn auch unter diesen Prinzipien zur Sicherstellung eines freien Datenflusses die einzigen Ausnahmen aufgezählt, die zur Durchberechnung des Grundsatzes berechtigen (§ 17 RL). Grundsätzlich ist eine Beschränkung des Datenflusses immer dann erlaubt, wenn der freie Datenverkehr dazu missbraucht wird, die geltenden Datenschutzbestimmungen eines Mitgliedstaates zu umgehen, so dass das im Teil II.

110 OECD, Explanatory Memorandum, N 68.

111 USA, CDN.

112 Id., a.a.O., N 65.

skizzierte Mindestmass an Schutz der Daten für die betroffene Person nicht mehr sichergestellt ist. Als typisches Beispiel wird der Wiederexport¹¹³ von einem Vertragsstaat in einen Drittstaat aufgeführt, dadurch soll verhindert werden, dass Daten über ein sog. "Ausflussrohr"¹¹⁴ in ein Territorium mit schwächerem oder gar keinem Datenschutz gelangen. Ferner, wenn wegen der speziellen Datennatur grundlegende Interessen des exportierenden Mitgliedstaates verletzt werden (z.B. Verbot des wirtschaftlichen Nachrichtendienstes, Art.273 StGB). Die allgemeine und generelle Formulierung der RL vermag das Problem des Wiederexportes klarer zu erfassen und zu lösen, als die KE.¹¹⁵

D. Teil IV.

Teil IV. (§ 19 RL) enthält Bestimmungen zur Implementierung der in den Richtlinien in Teil II. und III. niedergelegten Grundsätze. Dabei wird allgemein die Einführung eines entsprechenden nationalen Datenschutzgesetzes empfohlen und dessen inhaltlicher Rahmen generell umrissen wie z.B durch

- die Einführung von Kontrollmechanismen (Individualkontrolle, Selbstkontrolle, Verhaltenskodex für DV-Personal);
- Vorschriften zur Verwirklichung der Individualrechte sowie über administrative Rechtshilfe und Konsultationen der verantwortlichen Stellen;
- Aufnahme strafrechtlicher, zivilrechtlicher und verwaltungsrechtlicher Bestimmungen und Massnahmen;
- Vorkehrungen gegen ungerechtfertigte Diskriminierungen wie z.B. Ungleichbehandlung aufgrund der Nationalität, Wohnsitz, Rasse etc.

E. Teil V.

a) Internationale Zusammenarbeit (§§ 20 - 22 RL)

Neben den Prinzipien zur Regelung des grenzüberschreitenden

113 D.h. dass zumindest ein Export vom Ursprungsland in ein anderes Mitgliedsland bereits vollzogen wurde.

114 D.h. ein Mitgliedsstaat mit larger Gesetzgebung; in der KE unter Problemen des Exportes als blosser Transitstaat geregelt.

115 Vgl. vorne, S. 260f., OECD, Explanatory Memorandum, N 67.

Datenflusses sind auch die Formen der gegenseitigen Rechtshilfe und Zusammenarbeit der Behörden der Mitgliedsstaaten für die Betrachtungen zum Datenschutz auf internationaler Ebene bedeutsam.

Die innerhalb dieses Teiles vorgesehene Zusammenarbeit der Behörden der Mitgliedsstaaten bleibt hinter derjenigen der KE zurück: Die KE ist ausführlicher und weitergehend, als die bloss summarischen Vorschriften der Richtlinien. So beschränken sich die RL einerseits auf die Sicherstellung des Informations- und Erfahrungsaustausches über die Anwendung der RL und deren Ausprägung in nationalen Gesetzen in Form von Gesetzesnormen, Verordnungen oder Verfügungen angesichts der komplexen und verwirrenden Lage nationalstaatlich unterschiedlicher Konzeption, andererseits auf die Gewährung gegenseitiger Rechtshilfe bei Verfahrensfragen und der damit verbundenen wechselseitigen Information über spezielle Regeln und Entscheidungen. Unter der Rechtshilfe bei Verfahrensfragen ist die Hilfe für natürliche Personen bei der Geltendmachung ihrer aus dem Datenschutzrecht fliessenden Individualrechte zu verstehen, falls die Datensubjekte ihren Wohnsitz in einem der Mitgliedstaaten haben.

Ebenfalls unter die Rechtshilfe subsumiert wurde die Vorschrift, dass formale Bestimmungen (d.h. administrative Verfahrensnormen) zu vermeiden sind, die den freien Datenfluss unnötig beeinträchtigen könnten. Dies zielt darauf ab, die im Zusammenhang mit dem grenzüberschreitenden Datenverkehr stehenden Verfahren zu vereinheitlichen, eingeschlossen die Ueberwachung und Kontrolle, und, falls notwendig, die Zulässigkeitsvoraussetzungen zur Durchführung der Datenverarbeitung.

In den RL fehlen hingegen Vorschriften, die das Funktionieren der Rechtshilfemechanismen konkretisieren, wie z.B. eine Lösung der Frage der Kostenlast bei der Rechtshilfe, Art und Form der Unterstützung der Datensubjekte bei der Geltendmachung ihrer Kontrollrechte (z.B. kostenlose Uebersetzung durch einheimische Behörden bei Auskunfterteilung, weil diese aufgrund der gegenseitigen Informationen dazu befähigt sind), nähere Spezifikation der mit der Rechtshilfe verbundenen Erfordernisse (z.B. Rechtshilfegründe, Abweisungsgründe). Ungelöst bleibt auch die Frage des potentiellen Missbrauches durch

die Behörden aufgrund der internationalen Zusammenarbeit erlangten Kenntnisse.

Die RL schweigen auch über die Form und Art der Rechtshilfe bei integrierten Datennetzen, sowie über die gegenseitige Vollstreckung von Entscheidungen, die in anderen Mitgliedsstaaten gefällt wurden.

b) Gesetzes- und Zuständigkeitskonflikte ¹¹⁶

Die Richtlinien empfehlen den Staaten die Aufstellung von Prinzipien zur Bestimmung des anwendbaren Rechts bei grenzüberschreitenden personenbezogenen Datenflüssen sowohl für die nationale wie internationale Ebene (§ 22 RL). Mit der Schaffung von Kollisionsnormen auf nationaler Ebene besteht aber die Gefahr einer materiell- und formell-rechtlich divergierenden Ausbildung in den verschiedenen Mitgliedsstaaten. Diese nationalen Abweichungen könnten zu einem unbefriedigenden Resultat mit (Weiter- und Rück-) Verweisungen führen und das Datensubjekt bei der Wahrnehmung seiner Rechte belasten. Angesichts des unbestrittenen und global gleichgelagerten Schutzbedürfnisses der von der DV betroffenen Personen wäre es wünschenswert, wenn eine in allen Mitgliedstaaten einer Vereinbarung einheitliche, den gleichen Prinzipien folgende Bestimmung der Zuständigkeit und des anwendbaren Rechts erfolgen könnte.

F. Folgerung

Die OECD-Guidelines charakterisieren sich vor allem durch eine sehr ausführliche und detaillierte Regelung des grenzüberschreitenden Datenverkehrs, die derjenigen der KE überlegen ist. Die Richtlinien vermögen eine ausgewogene Lösung der gegensätzlichen Interessen von Datenschutz und freiem Datenverkehr anzubieten und erfüllen die in der Präambel gesteckten Postulate weitgehend. Ergänzungsbedürftig bleiben die RL hinsichtlich

- einer Differenzierung der Vorschriften (z.B. Zweckbestimmung) zwischen öffentlichem und privatem Bereich;
- einer externen Kontrolle;

116 Vgl. OECD, Explanatory Memorandum, N 74-76.

- der Gestaltung der Rechtshilfe und der internationalen Zusammenarbeit im Hinblick auf eine einfache Verwirklichung und Durchsetzung der Datenschutzprinzipien (Kontrollrechte) auf internationaler Ebene.

Schliesslich ist m.E. eine Lösung der möglichen Gesetzes- und Zuständigkeitskonflikte im grenzüberschreitenden Verkehr zur Durchsetzung der aus dem Datenschutz fliessenden Rechte dringend notwendig.

IV. Europäisches Parlament: Empfehlungen an die EG-Kommission und den EG-Rat

Auch das EG-Parlament ist seit 1976 damit beschäftigt, einen Parlamentsvorschlag zum Individualschutz auszuarbeiten, der sich vor allem auf die Datenverarbeitung bezieht und schliesslich in einem Richtlinienentwurf an die Kommission enden könnte. Im Bewusstsein, dass eine Richtlinie, die innerhalb der Europäischen Gemeinschaft nicht nur das Informationsgleichgewicht wahren, sondern auch einen effizienten Datenschutz und die Gesetzmässigkeit der Informationsverarbeitung sichern sollte, zwar notwendig ist,¹¹⁷ im Interesse der Realisierung des Datenschutzes auf internationaler Ebene sich jedoch nicht verschiedene internationale Vorgaben gegenseitig konkurrenzieren sollten, noch nebeneinander ins nationale Recht überführt werden können, hat die EG-Kommission beschlossen, "eigene Initiativen (Richtlinienentwurf) zurückzustellen, bis die endgültige Fassung einer Konvention des Europarates vorliegt."¹¹⁸

Aus diesem Grund verzichtet der Verfasser auf eine Besprechung des Wortlautes der Empfehlungen dieses Gremiums und verweist auf die aufgeführte Literatur.¹¹⁹

117 MEISTER, DS + DS 1/80, S. 11

118 So Kommissions-Vizepräsident Natali in der Sitzung des EG-Parlamentes vom 24. Sept. 1979, in: Official Journal (Anm. 5), S. 21: "we prefer to see how the situation develops in the council of Europe." (zit. Anm. 7, MEISTER, a.a.O., S. 16.).

119 Id., a.a.O.; TDR, Vol. 2, No. 2, 1979, S. 7ff.; (TDR, Vol. 2, No. 6, 1980, S. 15f.; CONRADI, DSWR 11/79, S. 247; STADLER, DS+DS 3/79 S. 169ff.

V. Schlussfolgerung

Die Konvention des Europarates stellt in der bestehenden Form als "non self executing convention" erst eine Vorstufe zu einer internationalen Lösung der mit dem grenzüberschreitenden Datenverkehr zusammenhängenden Probleme dar. Es fehlen vor allem materielle Normen, die konkret die internationalen Aspekte des Datenschutzes auf einheitliche und verbindliche Weise zu lösen vermögen. Dennoch ist m.E. die geleistete Arbeit und Bemühung hinsichtlich der Harmonisierung der nationalen Datenschutzrechte wie sie in der KE nun vorliegt nicht umsonst, da sie eine wesentliche Grundlage für ein zukünftiges internationales Rechtsregime zum grenzüberschreitenden Datenverkehr bildet. Die durch die Konvention bedingte Form hat für die Vertragsstaaten eine hemmende Wirkung. Man mag verschiedenster Auffassung über die Vorteile und Nachteile von bindenden oder nur empfehlenden Bestimmungen sein, Tatsache ist, dass mit verpflichtenden Verträgen ein höherer Harmonisierungsgrad erreicht wird, als mit der Aufstellung bloss zu beachtender Richtlinien. Allerdings stellt sich die Frage, welcher Weg zur Erlangung eines internationalen Rechtsregimes sich als optimal erweist und eingeschlagen werden soll. Richtlinien nach dem Muster der OECD bieten den Vorteil der Flexibilität und einer schnelleren Umsetzung in die nationale Rechtsordnung, da es dazu keines Ratifizierungsverfahrens bedarf;¹²⁰ insofern sind die OECD-Guidelines besser geeignet, in einer ersten Phase der Erfahrungssammlung auf dem Gebiet des grenzüberschreitenden Datenverkehrs eine Harmonisierung und Nivellierung des Schutzniveaus in dem in den Grundprinzipien festgelegten Mass zu erreichen.

Wichtig ist, dass die voneinander abweichenden Entwürfe einander nicht gegenseitig konkurrenzieren und die Datenschutz-Nationen in zwei Lager spalten, denn die bestehenden Entwürfe sind nicht ausgereift und vermögen noch keine vollständige Lösung anzubieten. Es ist auch nicht denkbar, dass "mehrere internationale Vorgaben nebeneinander in nationales Recht überführt werden."¹²¹

120 MEISTER, DS+DS 1/80, S. 15.

121 Id., a.a.O, S. 15; vgl. auch DS+DS 4/80, S. 239.

III. TEIL: SCHLUSSFOLGERUNG UND LOESUNGSVORSCHLAEGE

§ 11 DIFFERENZIERUNG DES GRENZUEBERSCHREITENDEN DATENVERKEHRS HINSICHTLICH EINER RECHTLICHEN REGELUNG

Vom Standpunkt eines Gesetzgebers ist innerhalb des grenzüberschreitenden Datenverkehrs grundsätzlich zwischen Export und Import personenbezogener Daten zu unterscheiden. Diese Differenzierung folgt aus den mit Export und Import verbundenen, unterschiedlichen Rechtsfolgen für das betreffende Datum bzw. Datensubjekt, das zum Inland einen bestimmten Konnex aufweist (Binnenkonnex, d.h. die Beziehung eines Datums, zum Staat, in dem es seinen Ursprung hat).

I. Export

Beim Export verlassen personenbezogene Daten den Rechtsbereich desjenigen Landes, in dem sie in einer Datensammlung gespeichert oder irgendeinem Verarbeitungsvorgang (automatisierter oder manueller) Natur unterzogen wurden. Mit Eintritt in ein anderes nationales Hoheitsgebiet ist das anwendbare Recht des entsprechenden Transit-¹ oder Destinationslandes ² massgeblich. Bezogen auf das Datum, sind somit Export und Import komplementär.

Unter Export personenbezogener Daten ist jede Form des Verlassens eines Rechtskreises und der damit zusammenhängende Uebertritt in einen andern Hoheitsbereich zu verstehen, gleichgültig, ob dieser Vorgang auf elektronische bzw. elektromagnetische Art über private oder öffentliche Telephonleitungen, Satellit, Funk oder auf manuelle Weise mittels Transportieren von Bändern, Disketten, Lochkarten, Disks, Computerausdrucken oder andern Speichermedien erfolgt. Rechtlich ent-

1 Vgl. nachfolgend, S. 293.

2 Vgl. Import, hinten S. 289ff.

scheidend für das Datum bzw. Datensubjekt ist, dass für seinen Schutz ein anderes Recht anwendbar ist, und nicht die Art und Weise der Uebertragung.³

Datenschutzrechtlich nicht relevant ist die nachfolgend (für Export und Import⁴) skizzierte Unterscheidung⁵ zwischen der Ausfuhr von Daten inländischer Datenträger⁶ bzw. Verarbeitungsmedien und dem Zugriff auf inländische Datenbanken vom Ausland her.⁷ Die Ausfuhr von inländischen Daten auf ausländische Verarbeitungsmedien

3 Dass sowohl die manuelle als auch automatisierte Uebertragung von Daten in einen andern Rechtskreis für den Betroffenen negative Folgen haben kann, ist unbestritten.

4 Vgl. nachfolgend S. 286 und S. 290.

5 Die hier angestellte Unterscheidung ist auch nicht Informatikspezifisch; eine auf die Informatik ausgerichtete Unterscheidung der Anwendungsmöglichkeiten lässt (auch hinsichtlich zukünftiger Satellitenübertragungen) folgende, in der Praxis oft nur schwer vollziehbare Trennung zwischen zwei Formen zu:

- Datentransfer umschliesst die Anwendungen, "die vom direkten Zugriff zu weit entfernten Daten oder Dateien bis zum Uebertragen grosser Datenmengen oder Dateien reichen und Anwendungen einschliessen, die man gelegentlich unter dem Sammelbegriff 'elektronische Post' zusammenfasst." (KIMMICH/SIMON, S. 51) Unter dem Begriff des 'electronic mail' werden auch die Faksimileübertragungen sowie das Fernkopieren subsumiert. Als Anwendungsbeispiel eines internationalen Datentransfers können die Uebermittlungen von Daten zwischen Kreditunternehmen genannt werden, aber auch Flugreservationssysteme etc.
- Beim Lastverbund handelt es sich nach KIMMICH/SIMON (a.a.O.) "um die Koppelung der Rechen- und Verarbeitungskapazität von Datenverarbeitungssystemen" wie sie heute schon bei vielen Rechenzentren mit nahe beieinanderstehenden Datenverarbeitungssystemen ausgeführt wird. Mangels grosser Uebertragungsgeschwindigkeiten und -kapazitäten zwischen weit entfernten Systemen wird diesem Anwendungsbereich mit der Entwicklung von Satellitenübertragung (und damit hoher Uebertragungskapazitäten [z.B. 1,544 Megabits/Sekunde]) noch erhöhte Bedeutung zukommen, so dass z.B. im Ausland lokalisierte Computer als Ersatz für ausgefallene Systeme arbeiten können oder bei internationalen Firmen eine bessere Auslastung der DV-Kapazität stattfinden kann durch Ausnützung der Zeitverschiebung und damit verbundene Minimal- oder Schwachbelastungen.

6 Bzw. Dateien, Datensammlungen.

7 Und umgekehrt: auf ausländische Datenbanken vom Inland her, vgl. hinten, S. 291.

oder Datensammlungen kann sowohl in der Form des Datentransfers⁸ als auch des Lastverbundes⁹ erfolgen. Der direkte Zugriff auf Datenbanken vom Inland respektive Ausland¹⁰ her ist eine spezielle Verarbeitungsart, die gemäss Umschreibung von KIMMICH/SIMON¹¹ in die Kategorie des Datentransfers einzureihen ist. In beiden Fällen findet ein Datenexport statt, der weder zwischen herkömmlicher und automatischer Uebermittlungsart im allgemeinen, noch den verschiedenen Formen der computerisierten Uebertragung im besondern, eine materiellrechtlich differenzierte Behandlung erfordert.

1. Ausfuhr von Daten aus inländischen Datensammlungen auf ausländische Verarbeitungsmedien oder Datensammlungen

Bei der Ausfuhr von Daten geht der Transfer ins Ausland vom Inhaber, "Halter" einer Datensammlung oder einem Betreiber der inländischen Datenverarbeitungsanlage aus. Ohne seine entsprechenden Handlungen ist kein Export personenbezogener Informationen möglich. In der Regel wird es sich bei Uebermittlungen dieser Art um grössere Datenmengen¹² handeln. Die Uebertragung lässt sich auf manuelle Art¹³ oder durch automatisierte Verfahren¹⁴ vollziehen.

Dieser Export kann nun entsprechend dem spezifischen Tätigkeitsbereich des ausländischen Benützers entweder dauernder Natur sein (z.B. bei Weitergabe von Planungsdaten, Konsolidierung von Planungsdaten verbundener Unternehmen) oder nur zur Ausführung bestimmter Arbeitsschritte im Ausland (z.B. zur Benützung spezieller Software/Hardware oder zur Verknüpfung mit Angaben, die in ausländischen Systemen gespeichert sind) erfolgen, mit anschliessender Wiedereinfuhr der

8 Vgl. oben, Anm. 5.

9 Vgl. oben, Anm. 5.

10 Vgl. nachfolgend, S. 287f. (Export) und S. 291f. (Import).

11 KIMMICH/SIMON, S. 51; vgl. oben Anm. 5.

12 Im Gegensatz zum Zugriff, wo die ausgeführte Datenmenge in der Regel kleiner ist, weil der Benutzer (im Ausland) es vorzieht, die (inländische) Datenbank zu benutzen und auf den Aufbau einer eigenen Datenbank mit denselben Daten zu verzichten.

13 Mittels Ueberbringen von Disks, Tapes, Disketten, Computerlisten, -ausdrucken, etc.

14 Ueber Telefonleitungen, Satellit, Funk etc.

verarbeiteten Daten. Im letzteren Falle ist bei der rechtlichen Ausgestaltung darauf zu achten, dass das bei einem beabsichtigten Wiederimport zu durchlaufende Verfahren nicht zu schwerfällig¹⁵ geregelt wird, da dies eine hemmende Wirkung auf den Export für Spezialverarbeitungen ausüben und u.U. protektionistische Züge annehmen könnte. Auch der umgekehrte Fall der Ausfuhr, wo Daten, die keine Inlandsbeziehung aufweisen, nur zur Durchführung spezieller Verarbeitungsvorgänge importiert wurden, ist eine Form des Datenexportes; aber die Tatsache, dass diese personenbezogenen Informationen nur zwecks spezieller Verarbeitung eingeführt und danach wieder ausgeführt werden, ohne dadurch eine Beziehung zum Inland zu erhalten, erfordert m.E. eine rechtliche Sonderbehandlung i.S. des erleichterten Exportes.¹⁶ Diese Spezialbehandlung ist einerseits bedingt durch die Natur der modernen EDV, andererseits durch Wirtschaftlichkeitsüberlegungen, die für spezialisierte Verarbeitungsprozeduren mit kostspieligen Anwendungsprogrammen und entsprechenden Anlagen eine zentralisierte Verarbeitungsweise verlangen.

2. Zugriff auf inländische Datenbanken mit personenbezogenen Informationen vom Ausland her

Diese Exportart ist spezifisch für die elektronische Datenverarbeitung, welche eine dialogmässige Abfrage inländischer Datenbanken von Datenstationen im Ausland her erlaubt.

Die Handlung des im Inland befindlichen Inhabers der Datenverarbeitungsanlage ist hier dadurch charakterisiert, dass er nicht die Ausfuhr der Daten selbst vollzieht, sondern sie durch Erstellung eines entsprechenden Benutzerprofils (und den Aufbau der Datenbank für dialogmässige Bearbeitung) ermöglicht. Der ausländische Benutzer eines Terminals erhält dadurch die Möglichkeit, auf die personenbezogenen Informationen im Inland zuzugreifen, von diesen auf Datenstationen im Ausland Kenntnis zu nehmen¹⁷ und sie entsprechend zu

15 Z.B. mit strengen Genehmigungserfordernissen für den Einzelfall.

16 Vgl. hinten, S. 362.

verarbeiten. Auf diesem Wege findet selten eine Uebertragung eines ganzen Datenbestandes statt, es wird vielmehr eine "punktuelle" Uebermittlung bzw. ein repetitiver Transfer bestimmter Einzeldaten vollzogen. Durch den Zugriff erlangt der ausländische Benutzer die virtuelle Verfügungsgewalt über alle Angaben der Datenbank (wobei diese aber von deren Struktur abhängig ist). Auch hier ist die Schaffung der Möglichkeit des Exportes vom Inhaber der Datenbank abhängig, die Aktualisierung des Exportes hingegen vom Benutzer im Ausland. Der Benutzer im Ausland hat beim Zugriff auf Datenbanken in der Regel nicht die Absicht, mit den durch Zugreifen erlangten Daten selbst eine Datenbank aufzubauen, weil ihm der Unterhalt und das Führen einer solchen Datenbank nicht wirtschaftlich oder nicht zweckmässig erscheint.

De facto stellt der Zugriff auf den Datenbestand einer im Inland gelegenen Datenbank eine Ausfuhr der gespeicherten Informationen dar, die aber im Rahmen des Exportes keine unterschiedliche rechtliche Behandlung gegenüber dem vorgenannten Fall der Ausfuhr¹⁷ rechtfertigt; im Gegenteil: die Identität des Resultates, d.h. des Uebertritts der Daten in einen anderen Rechtskreis legt sogar bei einer gesetzlichen Regelung des Exportes eine 'gesonderte' Gleichbehandlung¹⁹ der beiden Tatbestände nahe, da bei unterschiedlichen Rechtsfolgen Rechtsunsicherheit infolge Abgrenzungsschwierigkeiten entstehen könnte.

Für die Ausgestaltung der Vorschriften des inländischen Rechts ist erheblich, ob der ausländische Benutzer durch den direkten Zugriff ein Verfügungsrecht (Recht auf Aenderung, Nachführung, Löschung, etc.) über die Daten hat. Besitzt er kein Verfügungsrecht, findet lediglich ein Export von Angaben statt, ohne dass der Datenbestand durch die Ausfuhr eine Aenderung erfährt, weil nur eine Kopie der Informationen ausgeführt wird; ist dem Exportierenden hingegen das Verfügungsrecht über die Daten eingeräumt, kann er gleichzeitig

17 Auch ein Ausdruck der so erhaltenen Daten ist grundsätzlich möglich.

18 Vgl. vorne, Nr. 1, S. 286f.

19 Vgl. Oesterreich: §§ 32, 34 Abs.1 und §§ 33, 34 Abs.2 DSG.

auch Daten löschen, ergänzen oder ändern etc., was auch negative Auswirkungen²⁰ auf den Betroffenen haben kann. Hier wäre grundsätzlich eine Formel angebracht, die vorschreibt, dass von allen exportierten Daten mit Binnenkonnex eine Kopie zurückbehalten werden muss: Dies diene nicht nur der Kontrolle, sondern ebenfalls der Vermeidung von Persönlichkeitsverletzungen durch ein Löschen, Mutieren und Ergänzen von Angaben.

II. Import

Im Unterschied zum Export, bei dem jeder Gesetzgeber bestrebt ist, sich eine Durchgriffsmöglichkeit zu schaffen, um bei potentiellen Gefährdungen, die beim Verlassen des eigenen Rechtskreises für personenbezogene Daten auftreten können, das entsprechende Schutzdispositiv²¹ wirken zu lassen, gelangen beim Import die Daten in den Anwendungs- und Geltungsbereich der eigenen, vom Gesetzgeber selbst geschaffenen Rechtsordnung. Durch den Eintritt der Informationen in den Hoheitsbereich des Inlandes unterstehen diese automatisch dem Schutz der entsprechenden Gesetze, unabhängig, auf welche Art²² diese in den eigenen Hoheitsbereich gelangt sind. Entscheidend ist, dass die Daten im Inland verarbeitet werden, so dass der Importierende bzw. der inländische Datenverarbeiter sich beim Umgang mit den eingeführten Daten an die gleichen Vorschriften zu halten hat, wie bei der Bearbeitung von Angaben aus dem Inland. Diese Tatsache hat zur Folge, dass kaum spezielle Schutz- oder Abwehrvorkehrungen gegen den Datenimport geschaffen werden müssen, da die geltenden Voraussetzungen über die Zulässigkeit der Datenverarbeitung (falls solche existieren)²³ eine mit Verletzung der Persönlichkeit verbundene Verarbeitung importierter Daten verhindern würden.

20 So kann u.U. das "Nicht-gespeichert-Sein" ebenfalls eine Persönlichkeitsverletzung verursachen, z.B. bei positiven Angaben, die die Kreditwürdigkeit bestätigen.

21 Vgl. vorne, S. 220.

22 Automatisiert (computerisiert) oder manuell.

Im Zusammenhang mit dem postulierten freien transnationalen Datenfluss innerhalb eines Konventionsgebietes ist jedoch für den Fall des Wiederausports u.U. die Einführung einer Genehmigungspflicht ratsam. Auch hier drängt sich analog zum Export²⁴ die Unterscheidung zwischen der Einfuhr von Daten ausländischer Datenbanken auf inländische Datensammlungen und Systeme einerseits und dem Zugriff auf ausländische Datenbanken vom Inland her andererseits auf; sie sollte m.E. auf die Beurteilung des Importes als solchen jedoch keine materiellen Auswirkungen haben.²⁵

1. Einfuhr von Daten ausländischer Datensammlungen auf inländische Datenverarbeitungssysteme

Beim Import werden Daten, die vom Inhaber einer Datenbank im Ausland exportiert werden, vom inländischen Benutzer eines Datenverarbeitungssystems eingeführt, was bedeutet, dass er u.U. das System auf den Empfang dieser Informationen vorzubereiten hat. Auch hier handelt es sich im Gegensatz zum Zugriff in der Regel um die Uebertragung grösserer Datenbestände oder sogar ganzer Datenbanken (z.B. bei Konsolidierungen). Die Daten werden im Regelfall in den existierenden Datenbestand integriert und gespeichert; vor allem dann, wenn die Angaben zu dauerndem Zweck eingeführt werden. Die Informationen können aber auch bloss vorübergehend, zur Vornahme spezieller Verarbeitungsschritte (z.B. im Rahmen des Lastverbundes), importiert werden: für diese Fälle sollte sowohl das Einfuhr- wie auch das Ausfuhrprozedere eine liberale, unkomplizierte Ausgestaltung²⁶ erfahren, sofern die

23 Existieren keine Zulässigkeitsvoraussetzungen zur Datenverarbeitung, ist ein solches Abwehrdispositiv gegen den Import von Daten vorzusehen, ansonsten die Gefahr eines data havens aktuell werden kann.

24 Vgl. vorne, S. 285.

25 Vgl. vorne, S. 286.

Daten keine Binnenbeziehung (d.h. Verknüpfung mit Ursprungsdaten) aufweisen und mit dem nachfolgenden Export keinerlei Persönlichkeitsverletzungen zu befürchten sind. In diesem Falle ist z.B. eine Vorschrift zu einem genehmigungsfreien Export denkbar, falls die zu speziellen Verarbeitungszwecken importierten Daten wieder in das Ursprungsland zurückgeführt werden sollen: damit könnte man das Prinzip des freien transnationalen Informationsflusses in beschränktem Masse auf staatlicher Ebene erfüllen.

Im Gegensatz zum Zugriff auf Datenbanken, der als typische Erscheinungsform der ADV nur automationsunterstützt erfolgen kann, ist die Einfuhr von Daten sowohl manuell (d.h. durch Uebersendung von Disks, Tapes, Lochkarten etc.) als auch automatisiert (über Leitungen, Satellitenverbindungen) zu bewerkstelligen.

2. Zugriff auf ausländische Datenbanken vom Inland aus

Beim Zugriff auf ausländische Datenbanken wird der inländische Benutzer in die Lage versetzt, über im Inland befindliche Terminals auf den Datenbestand einer im Ausland gelegenen Datenbank zu greifen. Art und Umfang der Daten, die mittels Datenfernverarbeitung abgerufen werden, wird vom inländischen Benutzer der Datenbank bestimmt.

Analog dem Export ist der im Inland befindliche Zugriffsberechtigte i.d.R. nicht bestrebt, mit den importierten Daten eine neue Datenbank im Inland aufzubauen, sondern er zieht es vor, lediglich auf die Daten zum Zwecke ihrer Verarbeitung und Nutzung zuzugreifen, ohne selbst Aufwendungen für Unterhalt und Verwaltung der Datenbank leisten zu müssen.²⁷

In Wirklichkeit ist aber auch der Zugriff auf ausländische Datenbanken und die damit verbundene Ausgabe der personenbezogenen Informationen auf einer inländischen Datenstation eine Einfuhr von Daten, die rechtlich keine unterschiedliche Behandlung gegenüber dem Import

26 Vgl. vorne, S. 287 und hinten, S. 362, 367.

27 Dies unterstreicht nochmals, dass in der Praxis die Entscheidung zwischen Zugriff auf Datenbanken und der Einfuhr grosser Datenmengen bzw. ganzer Dateien von wirtschaftlichen Faktoren und Zweckmässigkeitsüberlegungen abhängig ist.

größerer Datenmengen rechtfertigt, ansonsten Umgehungsmöglichkeiten eröffnet werden könnten. Vielmehr ist es angebracht, beide Fälle gleich einzustufen und unter dem generellen Tatbestand der Dateneinfuhr zu regeln - eine rechtliche Differenzierung zwischen diesen beiden Importarten könnte höchstens zu Abgrenzungsproblemen und starren, nicht entwicklungsfähigen Begriffsbestimmungen führen.

Dagegen ist eine Unterscheidung in der rechtlichen Ausgestaltung zwischen einem Zugriff mit Verfügungsgewalt und einem ohne diese Machtbefugnis über die Daten angebracht. Ist der Benutzer autorisiert, den Bestand der Datensammlung durch Mutationen, Ergänzungen, Löschungen etc. zu verändern, sollte er zum Vollzug eines mit einem Individualrecht geltend gemachten Anspruchs verpflichtet sein. Hat er aber nur die Möglichkeiten des blossen Zugriffes, ohne gestaltend in den Datenbestand eingreifen zu können, beschränken sich seine Pflichten in bezug auf die Erfüllung von Individualrechten auf die Weiterleitung solcher Ansprüche an die für die Datenbank verantwortliche Stelle im Ausland.

III. Transit

Im Zusammenhang mit Export und Import können Daten auf Uebermittlungsmedien und -trägern durch Drittländer bzw. den Weltraum (bei Satellitenübertragungen) übermittelt werden, ohne einem speziellen Verarbeitungsvorgang unterzogen zu werden. Es ist aber innerhalb eines Datennetzes auch möglich, dass die Informationen zusätzlich zum Passieren von Leitungen und Uebertragungsmedien auch durch Datenverarbeitungssysteme laufen und von der Steuerungssoftware des Netzwerkes weiter- bzw. an die richtige Adresse geleitet werden; dabei kann es vorkommen, dass die übermittelten Daten zwischengespeichert werden, falls eine Destinationsstelle nicht aktiv ist. Die Daten durchlaufen in diesen Fällen sog. "transparent path's",²⁸ ohne dass sie in ihrer Substanz irgendeine Veränderung erfahren.²⁹ Die Daten können somit u.U. verschiedene nationale Hoheitsbereiche durchlaufen und potentiell mehreren Rechtsordnungen unterstehen. Theoretisch und praktisch sollte ein solcher Transit von Daten durch verschiedene nationalen Rechtsordnungen keine Auswirkungen auf das Schutzgut eines

Datenschutzgesetzes hinterlassen, da die Daten diese Territorien in deren Leitungsstrecken i.d.R. ungestört passieren; infolge der neuesten Uebermittlungstechnologien³⁰ ist der Transitweg von Daten oft weder im Voraus noch hinterher feststellbar. Erfolgt aber eine Störung der Uebermittlung auf einer Transitstrecke, so ist normalerweise das Recht desjenigen Landes anwendbar, in dem die Störung erfolgt ist, d.h. gemäss Territorialprinzip entscheidet das materielle Recht des Begehungsortes,³¹ ob eine Persönlichkeitsverletzung vorliegt oder nicht, und - falls eine solche zu bejahen ist - wird sie nach diesem Recht beurteilt. Zwar erscheint es als grundsätzlich möglich, in die Uebermittlungsvorgänge einzugreifen, doch kann die Ausnützung eines solchen Eingriffs in der Praxis durch die Chiffrierung der übertragenen Daten vereitelt werden. Die heutigen Verschlüsselungsmethoden³² erlauben eine sehr hohe Sicherheit³³ der Daten, so dass es kaum zu einer Persönlichkeitsverletzung kommen kann, falls die Informationen verschlüsselt übertragen werden.³⁴

28 Vgl. vorne, S. 80 Anm. 116.

29 Die Adresse der Daten kann von der Steuerungssoftware beim Durchlaufen dieser Steuerungsstellen geändert werden, dies erfolgt meist auf einem 'label' (Adressetikette); die Grundsubstanz des Datums bleibt aber unangetastet - es drängt sich hier der Vergleich mit einem Paket, dessen Etiketten mehrmals geändert werden müssen, auf: der Inhalt des Paketes bleibt bei diesen Vorgängen ebenfalls unangetastet.

30 Z.B. packet switching.

31 Lex loci delicti commissi.

32 Vgl. STRUEBY, S. 136: Chiffrierstandards des NBS; ferner National Bureau of Standards (NBS): NBS-DES (Data Encryption Standard von 1977).

33 Absolut kann sie nicht sein, da jedes System zu durchbrechen ist: Ein Verschlüsselungssystem, das z.B. 1000 Jahre zum Durchbrechen eines Schlüssels bei Vornahme und Berechnung einer Variante pro Sekunde benötigt, kann innerhalb eines Jahres mit 1000 Minicomputern geknackt werden. Die Sicherheit kann dennoch als hoch eingestuft werden, weil ein Durchbrechen dieses Schlüssels aufgrund des Verhältnisses von benötigtem Aufwand und resultierendem Nutzen bzw. Profit nicht mehr interessant erscheint.

34 Hieraus wird auch der Stellenwert der Datensicherung beim internationalen Datenaustausch ersichtlich.

Aufgrund der zunehmenden Verflechtung und der stetigen Ausdehnung der Datennetze muss eine rechtliche Regelung auf diese systeminternen, informationellen Abläufe Rücksicht nehmen, da sonst das Funktionieren solcher Netzwerke verunmöglicht oder blockiert werden kann und damit das Postulat des freien internationalen Datenflusses unerfüllbar bleibt. M.a.W. die mit einem Transit von Daten im Zusammenhang stehende Ein- und Ausfuhr von Angaben sowie eine eventuell damit verbundene Zwischenspeicherung darf nicht unter die allgemeinen gesetzlichen Tatbestände von Ein- und Ausfuhr fallen, auch wenn dabei ein Verarbeitungsvorgang im Zusammenhang mit der systemtechnischen Steuerung der Datenflüsse vorhanden ist. Vielmehr wäre hier eine Ausnahmebestimmung vorzusehen, die den besonderen Umständen Rechnung trägt und eine Abgrenzung vornimmt.

Die mit der Steuerung und Lenkung der Daten auf ihrem Transit verbundenen Verarbeitungsschritte müssen gegenüber den Vorgängen abgegrenzt werden, welche ein Bestandteil oder Ausführungsschritt einer Verarbeitung von Daten darstellen.

Eine Lösung dieser Frage sollte allerdings nicht auf einzelstaatlicher Ebene angestrebt werden, da sie einerseits national abweichende Ausprägungen erfährt und die Transparenz der anwendbaren Datenschutznormen vereiteln würde; andererseits würden unterschiedliche oder fehlende Sanktionen gegenüber Eingriffen in den Datentransit die Bildung von Datenoasen fördern. Die Klärung dieser Frage ist ein typisches Beispiel für die grundsätzliche Notwendigkeit eines internationalen Rechtsregimes und dessen potentielle inhaltliche Ausprägung; m.a.W. die vordergründige Aufgabe einer internationalen Vereinbarung sollte darin bestehen, einzelstaatlich nicht befriedigend lösbare Probleme auf internationaler Ebene einheitlich zu regeln, so dass das nationale Recht sich in diesen Bereichen damit begnügen kann auf die entsprechenden völkerrechtlichen Vereinbarungen zu verweisen.

§ 12 DAS SOG. "CONFLICT OF LAW"-PROBLEM BEIM GRENZUEBERSCHREITENDEN DATENVERKEHR. DIE SICH BEI VORLIEGEN VERSCHIEDENER DATENSCHUTZGESETZE BZW. BEI DEREN FEHLEN ERGEBENDEN PROBLEME.

Aus der Existenz unterschiedlicher Datenschutzgesetze bzw. wegen des Fehlens von Datenschutznormen in bestimmten Ländern, entsteht die Problematik des "transborder data flows". Dieser Problemkreis stellt sich allerdings nur für diejenigen Länder, die eine eigene Datenschutzgesetzgebung besitzen und sich um den Schutz der Persönlichkeit gegen die Gefährdungen im Zusammenhang mit der Bearbeitung von personenbezogenen Informationen bemühen. Die Optik des nationalen Gesetzgebers zur Lösung und Verwirklichung des Persönlichkeitsschutzes beim grenzüberschreitenden Datenverkehr ist dabei grundsätzlich anders ausgerichtet als diejenige einer internationalen Institution, die das innerhalb eines Verbundes mehrerer, mit unterschiedlichen Datenschutzgesetzen ausgestatteten Mitgliedstaaten anwendbare Recht bestimmen soll, falls ein persönlichkeitsverletzender Verarbeitungsvorgang stattfindet. In einem solchen, auf einem völkerrechtlichen Vertrag beruhenden Verbund von Staaten, die alle eigene nationale Datenschutzgesetze entwickelt haben, stellt sich das sog. "conflict of law"-Problem, d.h. die Frage, welches nationale Recht und welcher Gerichtsstand zur Anwendung kommen soll, falls aus der Bearbeitung von Daten im Ausland eine Persönlichkeitsverletzung resultiert.

I. Auf nationaler Ebene

1. Kollisionsprobleme

Für den nationalen Gesetzgeber bringt der grenzüberschreitende Datenverkehr nicht nur einen Wechsel des Hoheitsbereiches für Daten über Personen, sondern gleichzeitig auch das Problem der Entscheidung eines potentiellen Gesetzeskonfliktes bei der Verletzung dieser Daten im Ausland. Eine Kollision verschiedener Rechtsordnungen kann ihre Ursache in zwei gegensätzlichen Ausgangspunkten haben:

A. Ueberlappungen

Es ist denkbar, dass eine Kollision daraus resultiert, dass zwei Datenschutzgesetze das gleiche Problem unterschiedlich behandeln. Diese 'overlaps' entstehen meistens durch die Ausdehnung des Geltungsbereiches¹ eines nationalen Datenschutzgesetzes, die soweit führen kann, dass der Adressat in einen Konflikt über das anwendbare Recht gerät und seine normale Datenverarbeitungstätigkeit nicht mehr ausüben kann. Eine solche Blockierung kommt dann zustande, wenn die sich in ihrem Geltungsbereich überschneidenden Gesetze zueinander im Widerspruch stehen, so dass es für den Datenverarbeiter unmöglich wird, einen Bearbeitungsvorgang durchzuführen, ohne eines der Gesetze zu verletzen. Die Ausdehnung des Geltungsbereiches als Resultat eines zu stark ausgeprägten nationalen Schutzbereiches kann erhebliche negative Auswirkungen haben und ist m.E. grundsätzlich abzulehnen.

B. Gesetzeslücken

Auch die zur Ueberlappung konträre Erscheinungsform, die Gesetzeslücken, können eine Kollision von Gesetzen verursachen. Gesetzeslücken entstehen meist durch eine Beschränkung des Anwendungsbereiches auf bestimmte Personen,² auf bestimmte Verarbeitungsvorgänge³ usw., d.h. durch eine Begrenzung des Normendispositivs oder durch eine bloss partielle Regelung des Datenschutzes. Wenn ein Datenschutzgesetz den erwünschten, umfassenden Schutz entfalten soll, darf kein Bereich des Umganges mit geschützten Informationen ungeregelt bleiben, sondern muss vielmehr vermieden werden, dass die datenverarbeitenden Stellen über einfache Auswege ihre Tätigkeit in Gebiete, die einer andern Rechtshoheit unterstehen, verlagern, sei es, weil dort personenbezogene Daten keinem Schutz genießen, oder weil das

1 Z.B. Luxemburg, vgl. vorne, Anm. 253, S. 212/213, S. 242.

2 Z.B. nur Staatsbürger, nicht aber im Inland befindliche Ausländer (vgl. US-Privacy Act).

3 Z.B. nur automatische Datenverarbeitung.

inländische wie das ausländische Schutzsystem Schlupflöcher aufweisen, die gegenseitig ausgenützt werden können.⁴ Die national unterschiedliche Ausgestaltung von Datenschutzgesetzen bildet somit das grösste Risiko zur Entstehung von Gesetzeslücken und der damit verbundenen Umgehung eines Gesetzes.

C. Materiell widersprüchliche Gesetzesregelungen

Sowohl für den exportierenden, wie für den importierenden Datenverarbeiter im Ausland bilden sich Kollisionsprobleme, wenn die an seinem Sitz geltenden Bestimmungen im Widerspruch zu denjenigen des Auslandes⁵ stehen, so dass eine nach den Normen des Importlandes gesetzeskonforme Datenbearbeitung gemäss den Gesetzesbestimmungen des Exportlandes, infolge einer gegensätzlichen Regelung, rechtswidrig ist. In der Praxis kann dies auf nationaler Ebene ein Exportverbot bewirken, doch ist eine solche Erscheinungsform auch innerhalb von Konventionsstaaten, die sich zum freien Datenaustausch verpflichtet haben, möglich. Diese Fälle bilden jedoch eher einen Ausnahmefall, da die Problematik des Datenschutzes überall dieselbe ist.⁶

2. Reaktion des Gesetzgebers

In den bestehenden nationalen Datenschutzgesetzen ist keine ausdrückliche Kollisionsnorm zu finden, d.h. die Gesetze enthalten keine Bestimmung, die darüber Auskunft gibt, welches Recht und welcher Gerichtsstand bei einem internationalen Tatbestand anwendbar ist. Die Gesetze sagen nur, unter welchen Voraussetzungen die Verarbeitungshandlungen im Ausland einer Genehmigung unterliegen. Solche Regeln und Bestimmungen sind aber Normen des materiellen IPR: Sie unterwerfen einen Tatbestand, welcher sich auf dem nationalen Territorium er-

4 Vgl. SIEGHART, OECD-ICCP1, S. 227f. mit Beispiel.

5 D.h. des Importlandes bzw. des Exportlandes.

6 Ausserdem haben die Resolutionen (73) 22 und (74) 29 des Europarates die Grundvoraussetzung für eine Konvergenz der wichtigsten Problemkreise innerhalb der Mitgliedsstaaten geschaffen.

eignet und durch seine Beziehung zu einem ausländischen Tatbestand charakterisiert ist, einer speziellen auf den internationalen Status dieses Sachverhalts zugeschnittenen Lösung des nationalen materiellen Rechts. Es wird jedoch nur der Fall der nach inländischem Recht zulässigen Aus- bzw. Einfuhr geregelt, hingegen bleibt offen, welches Recht anzuwenden und welche Behörde dafür zuständig ist, wenn bei einem rechtmässigen Export infolge von Ueberlappungen, Lücken oder materiellen Widersprüchen eine Kollision mit einem andern Gesetz entsteht.

3. Notwendigkeit einer Kollisionsnorm?

Die nationalen Gesetzgeber haben sich bisher darauf beschränkt, eine Sicherung gegen Persönlichkeitsverletzungen im Ausland durch Schaffung eines Genehmigungssystems bzw. entsprechender Voraussetzungen für den genehmigungsfreien Export zu realisieren. Diese Sicherungsvorkehrung ist zweifelsohne wirksam, vermag indessen das Risiko von Persönlichkeitsverletzungen und damit zusammenhängende Ueberlappungen oder Lücken vorhandener Datenschutzgesetze nicht vollständig auszuschliessen, so dass es m.E. notwendig ist, in einem nationalen Gesetz für den Konflikt verschiedener Rechtsordnungen eine Lösung bezüglich ihrer Anwendbarkeit und derer Zuständigkeit vorzusehen.⁸

4. Die sich bei Vorliegen verschiedener Kollisionsnormen ergebenden Probleme

Da die Kollisionsnorm ihren Ursprung im innerstaatlichen, nationalen Recht hat,⁷ ist unvermeidbar, dass mehrere national unterschiedliche Kollisionsnormen entstehen. Eine Divergenz kann aber zu unpraktischen, lästigen Weiterverweisungen führen, die u.U. sogar mit dem Vorbehalt des 'ordre public' gegenüber einem an sich anwendbaren, fremden materiellen Recht enden könnte, so dass für alle am Verarbeitungsprozess Beteiligten (betroffene Person und die für die Datenver-

7 KELLER, S. 2.

8 Gl.M. SCHWEIZER, Computer und Recht, S. 111.

arbeitung im Ausland als Importierender oder Exportierender verantwortliche Stelle) ein ungünstiges Ergebnis resultiert. Da eine ergebnisbestimmte Anknüpfungsmethode wegen des imperativen Charakters der Kollisionsnormen⁹ abzulehnen und zu verneinen ist, hat die Uniformität bestimmter Kollisionsnormen eine gewisse Bedeutung.

Hinsichtlich der dargestellten Problematik erscheint die Tatsache, dass noch keine nationalen Kollisionsnormen in Datenschutzgesetzen erlassen wurden, als Positivum, da für deren Entwicklung eine gewisse Erfahrung aus dem Zusammenwirken verschiedener Datenschutzgesetze und ein Gedankenaustausch der nationalen Datenschutzbehörde wertvoll ist.

5. Schaffung einer Kollisionsnorm

Um eine gewisse Harmonisierung der Ausgestaltung nationaler Kollisionsnormen zu erreichen, scheint es mir sinnvoll, dass von einem internationalen Gremium¹⁰ diese Problemkreise anhand der Praxis und Erfahrung analysiert werden, um eine Harmonisierung der nationalen Kollisionsregeln (ev. in Übereinstimmung mit einer internationalen Konvention) zu erreichen. Dabei sollte angestrebt werden, dass das kompetenteste unter den konkurrierenden Rechten als anwendbar bezeichnet und zugleich die materiellrechtliche Gerechtigkeit am besten verwirklicht wird. Uebrigens muss auch eine Aussage über die örtliche und sachliche Zuständigkeit gemacht werden, da sonst eine langwierige vorfrageweise Auseinandersetzung um die Rechtsprechungshoheit für den zur Frage stehenden internationalen Tatbestand entstehen kann.

An dieser Stelle ist kein Raum, auf die materiellrechtliche Ausgestaltung mehrerer Normvarianten näher einzugehen: Dies sei den Kollisionsrechtlern überlassen; ich erachte aber eine Kompatibilität dieser nationalen Kollisionsnorm mit den Kollisionsbestimmungen eines internationalen Vertrages (gleichgültig ob der zur Frage stehende Staat Mitglied ist oder nicht), als sinnvolles Ziel des Gesetzgebers.

⁹ KELLER, S. 36f.

¹⁰ Z.B. Europarat oder OECD.

II. Auf internationaler Ebene

Die nachfolgend diskutierte Bestimmung des anwendbaren Rechts im Rahmen eines internationalen Abkommens ist eines der schwierigsten Probleme ¹¹ im Bereich des grenzüberschreitenden Datenverkehrs.

Eine Lösung dieser Frage würde nicht nur eine ausführliche Analyse der faktischen und rechtlichen Gegebenheiten bedingen und den Rahmen dieser Arbeit sprengen, sondern auch den Verfasser überfordern; er beschränkt sich deshalb - ohne einen speziellen Fall präjudizieren zu wollen - auf die Enumeration einiger Problempunkte und möglicher Lösungsaspekte, die Anlass zu weiteren, vertieften Arbeiten in diesem Themenkreis geben könnten.

1. Allgemeine Problematik des anwendbaren Rechts

Beim Versuch der Entwicklung einer supranationalen Datenschutzlösung stellt sich die Problematik des anwendbaren Rechts bei konkurrierenden Rechtsordnungen in einer andern Optik dar als auf nationaler Stufe. Die Zielsetzung ergibt sich hier aus einer Verflechtung verschiedenster Interessen:

- Primär ist auf diejenigen Staaten Rücksicht zu nehmen, die aufgrund ihres technisch-ökonomischen Entwicklungsstandes den Datenschutzgedanken bereits durch Gesetz institutionalisiert haben.^{12 13} Bei diesen sog. "Datenschutzstaaten" ist die Bereitschaft erkennbar, den aus der Datenverarbeitung erwachsenden Gefahren nicht nur auf nationaler, sondern auch auf internationaler Ebene entgegenzutreten und die sich aus der territorialen Beschränkung des Geltungsbereiches nationaler Datenschutzgesetze ergebenden Lücken mittels einer supranationalen Lösung zu schliessen; ausserdem zwingen die identische Interessenlage und wirtschaftlichen

11 Ähnlich STADLER, DS+DS 3/79, S. 171.

12 Dies sind hauptsächlich die Industriestaaten der westlichen Welt.

13 Bzw. bereits in der Phase der Legiferierung oder Ausarbeitung von Entwürfen stehen.

Handelsbeziehungen zu einem möglichst freien Informationsverkehr. Dieses Eigeninteresse der Datenschutznationen wird aber von national unterschiedlichen Nuancierungen und Bestrebungen geprägt, so dass die Schwierigkeit einer internationalen Lösung darin besteht, einen gleichen Ausgangspunkt oder eine ähnliche Behandlung des grenzüberschreitenden Datenverkehrs zu erreichen.

- Sekundär muss sich nun eine Anzahl dieser Datenschutzstaaten zu einem Interessenverbund zusammenfinden, um die Notwendigkeit multinationaler Kooperation durch Ausarbeitung und Verabschiedung internationaler Vereinbarungen in die Wirklichkeit umzusetzen. Innerhalb dieser Vereinbarungen gilt es nun, einerseits gewisse Unterschiede durch Harmonisierung auszugleichen, andererseits den national beschränkten und somit lückenhaften¹⁴ Schutzbereich durch Normen des Völkerrechts auf internationaler Ebene auszudehnen. Bei dieser Normsetzung bildet die Bestimmung des anwendbaren Rechts innerhalb eines geschlossenen Kreises von Mitgliedstaaten eines der Kernprobleme. Dabei ist nicht nur die Frage des anwendbaren Rechts und zuständigen Forums im Innenverhältnis (d.h. innerhalb eines geschlossenen Kreises von Signatarländern) festzusetzen,¹⁵ sondern auch das anwendbare Recht im Verhältnis zu andern Datenschutzstaaten, die nicht Mitglied des Interessenverbundes sind oder aber einem andern supranationalen Datenschutzverbund¹⁶ zugehören, der gleichgelagerte Bestrebungen mit einer materiell abweichenden Ausgestaltung verfolgt.

Dieser Gesamtheit von Staaten mit ausgeprägtem Datenschutzbewusstsein steht nun eine Kategorie von Ländern gegenüber, deren technisch-ökonomischer Entwicklungsstand bisher nur ein geringes oder

14 Vgl. z.B. vorne, S. 292ff.

15 Vgl. nachfolgend, Nr. 2, S. 302ff.

16 Zz.B. Staaten die OECD-Richtlinien beachten.

gar kein Datenschutzinteresse zu erzeugen vermochte. Gegenüber diesen Ländern sind Integrationsbemühungen nicht möglich, weil weder äquivalente Schutzgesetze existieren, noch ein Wille zur Kontrolle und Zusammenarbeit erkennbar ist. Die Ursachen für die mangelnde Kooperationsbereitschaft können verschieden sein, so z.B. fehlende Rechtsgrundlage, wirtschaftlich-technische Eigeninteressen, bewusste Ausnützung der Datenschutz-Situation (data havens) etc. Im Verhältnis zu diesen Staaten muss sich ein internationales Gremium darum bemühen, Abkommen mit diesen Ländern zu schliessen und, falls solche nicht erreichbar sind, mittels einer speziellen supranationalen Regelung¹⁷ den Datenfluss in diese Staaten entweder zu unterbinden oder durch Schutzmassnahmen und Vorprüfungen abzusichern. Daraus ergibt sich, dass die potentielle Ausnützung der die Persönlichkeit bedrohenden Möglichkeiten der Datenverarbeitung im gesetzessfreien Bereich des grenzüberschreitenden Datenverkehrs notwendigerweise Eingriffe des Gesetzgebers nach sich ziehen wird und die Freiheit des transnationalen Informationsaustausches generell beeinträchtigen kann.

2. Probleme und Lösungsmöglichkeiten der Bestimmung des anwendbaren Rechts im Rahmen einer internationalen Konvention

A. Lösungsansätze und -möglichkeiten

a) Ausgangspunkt

Als Ausgangspunkt der anschliessenden Betrachtungen müssen folgende Prämissen als gegeben erachtet werden:

- Die in Europa und Uebersee existierenden Nationen mit Datenschutzgesetzen, als potentielle Mitglieder einer künftigen völkerrechtlichen Konvention oder Vereinbarung, werden nicht bereit sein, auf ihre erst seit kurzem in Kraft stehenden nationalen Datenschutzrechte zugunsten eines harmonisierten internationalen Einheitsrechts zu verzichten. Den einen würde eine Einheitsregelung zu weit gehen, andern wiederum wäre sie zu minimal. Angesichts dieser Tatsache bleibt als möglicher Ausweg der Erlass eines Kerns von Vor-

schriften,¹⁸ die in einem nationalen Gesetz enthalten sein müssen, damit ein minimaler Schutzstandard durch jeden Mitgliedsstaat erfüllt wird. Daneben bestehende bereichsspezifische Regelungen sind von einer extrem nationaler Prägung, so dass für diese Bereiche ein Einheitsrecht illusorisch ist: Gerade diese bereichsspezifischen Bestimmungen verleihen einer nationalen Regelung das sie prägende Bild. Die Mitgliedsstaaten einer supranationalen Vereinbarung werden somit auf nationale wie auch auf internationale Tatbestände ihr einheimisches, nationales Recht zur Anwendung bringen.

- Dort, wo der grenzüberschreitende Datenverkehr nach einer spezifischen materiell- oder formellrechtlichen Regelung ruft, die auf der nationalen Ebene nicht die notwendige Wirkung zu erzielen vermag, sind rechtssetzende Normen zu erlassen, die aufgrund ihrer völkerrechtlichen Verbindlichkeit von jedem Signatarstaat beachtet¹⁹ werden müssen und dadurch eine einheitliche Lösung auf internationaler Ebene gewährleisten.²⁰
- Die als Vorbild gewählte Form einer Konvention²¹ geht vom Konzept der "geschlossenen Konvention" aus, d.h. als anwendbares Recht kann immer nur dasjenige eines Mitgliedsstaates in Frage kommen, so

17 Cf. hinten, Nr. 3, C., S. 324ff.

18 M.E. ist es nicht vorteilhaft, Minimalvorschriften in den Kern aufzunehmen, da die Einigung auf dem kleinsten gemeinsamen Nenner nur einen fragmentarischen Schutz bieten kann und das gegenseitige Vertrauen in die Wirksamkeit der Konvention unter den Mitgliedstaaten nicht unbedingt fördert. Besser wäre die Aufstellung von Maximalvorschriften mit der Möglichkeit der Einschränkung auf bestimmte Bereiche (z.B. Begrenzung des Anwendungsbereiches auf natürliche Personen), ohne dass Vorbehalte für nationale Abweichungen eine Konvention in ihrer Wirkungskraft zu stark einschränken.

19 Und u.U. in nationales Recht überführt werden müssen.

20 Z.B. die hier zur Diskussion anstehende Frage des auf internationale Verarbeitungsvorgänge anwendbaren Rechtes.

21 Ungeachtet der verschiedenen Ansichten über die angemessenste Lösung in Form einer Richtlinie i.S. der OECD oder als Konvention i.S. des Europarates (vgl. MEISTER, DS+DS 1/80, S. 9ff.). Letztlich ist aber die Verabschiedung eines "internationalen Rechtsregimes" i.S. eines völkerrechtlichen Vertrages Ziel einer internationalen Regelung, so dass das Vorbild der Konvention berechtigt ist.

dass Rechte von Drittstaaten von der Anwendung ausgeschlossen bleiben. Dies bedeutet gleichzeitig, dass als "Forum" nur die Gerichte und Behörden eines Mitgliedstaates bezeichnet werden können. Dieser geschlossene Kreis bildet die Voraussetzung für die Erfüllung eines minimalen Schutzstandards, welcher die Grundlage des gegenseitigen Vertrauens in die Wirksamkeit der Gesetzgebung (der einzelnen Vertragsländer schafft), so dass die Rechtsetzungskompetenz bzw. der Entscheid der nationalen Behörde eines Mitgliedstaates von den übrigen Konventionsländern auf der Grundlage dieses Minimalschutzes anerkannt und auch vollzogen wird.

Ausgehend von diesen Prämissen gilt es nun Anknüpfungspunkte zu entwickeln,²² welche das auf internationale Verarbeitungsvorgänge anwendbare Recht bestimmen. Ohne eine solche zwischenstaatliche Uebereinkunft besteht nicht nur die Unklarheit, wo beim internationalen Datenverkehr Ansprüche aus nationalen Datenschutzgesetzen geltend zu machen sind, sondern auch die Gefahr positiver bzw. negativer Gesetzeskonflikte.

b) Prinzip der Anknüpfung bzw. Frage der Zuständigkeit

Als mögliche Lösung bieten sich folgende Alternativen an:

- Die Bezeichnung eines anwendbaren Rechtes, unabhängig davon, welche Behörde dieses Recht zu beurteilen hat, oder die alleinige Bezeichnung einer zuständigen Behörde ohne Festlegung des anwendbaren Rechts. Diese Variante bietet den Nachteil, dass in Fällen des Auseinanderklaffens von "Jus und Forum" das die Rechtsfrage behandelnde Gericht ein ihm fremdes, ausländisches nationales Datenschutzrecht, einschliesslich dessen Normen über das Straf- und Verfahrensrecht, anzuwenden und zu beurteilen hat. Dabei kann aber der Vorbehalt des am Ort des zuständigen Richters geltenden "ordre public" die Anwendbarkeit des ausländischen materiellen Rechts verhindern.

22 Ich beschränke mich auf Anknüpfungspunkte für den privaten Bereich, weil der grenzüberschreitende Datenverkehr hier ein grösseres Ausmass hat und der öffentliche Bereich nach andern Grundsätzen zu beurteilen ist.

Bei einer Beschränkung der Kollisionsnorm auf die Bezeichnung des anwendbaren Rechts ohne Bestimmung des Gerichtsstandes bzw. auf die Festlegung nur der örtlichen Zuständigkeit wird deutlich, dass ein Auseinanderfallen von Gerichtsstand und anwendbarem Recht Probleme mit sich bringt, da die zuständige Behörde die Tendenz haben wird, die *lex fori*, d.h. das geltende einheimische Recht anzuwenden (sog. Heimwärtsstreben). Diese Lösung zur Bestimmung der örtlichen Zuständigkeit wird sich bei einer Befürwortung des Ubiquitätsprinzips aufdrängen, die eine Pflicht zur Behandlung der Ansprüche überall dort statuiert, wo eine Verarbeitungshandlung ausgeführt wurde.

- Die Nachteile des Heimwärtsstrebens können durch das vom angelsächsischen Recht verfolgten Prinzip der grundsätzlichen Einheit von Jus und Forum ^{23 24} weitgehend eliminiert werden. Diese Formel kommt der Tendenz zur Anwendung des Heimatrechts entgegen, da die Zuständigkeit *ipso iure* auch die Anwendbarkeit des nationalen materiellen und formellen Rechts der zuständigen Behörde begründet.

Das Lösungsprinzip der Einheit von Recht und Zuständigkeit hat den Vorteil, dass die vorfrageweisen Auseinandersetzungen um die örtliche Zuständigkeit, mit den ihnen anhaftenden Verweisungen oder möglichen Weiter- und Rückverweisungen, vermieden werden können; allerdings wird die Verwirklichung des Ubiquitätsprinzips Probleme bereiten. Trotzdem erweist sich dieses Prinzip für den internationalen Bereich des Datenschutzes ebenfalls als geeignet.

Ohne einen definitiven Entscheid fällen oder andere Formeln der Bestimmung der Zuständigkeit des IZPR und des IPR vorwegnehmen zu wollen, hat der Verfasser für die nachfolgenden Ausführungen zur Beurteilung möglicher Anknüpfungspunkte im privaten Bereich auf das

23 VISCHER, S. 634.

24 Dieses Prinzip ist verwirklicht im Haager Uebereinkommen über die Zuständigkeit der Behörden und das anzuwendende Recht des Schutzes von Minderjährigen vom 5. Oktober 1961.

Prinzip der Einheit von Jus und Forum abgestellt, jedoch im Bewusstsein des Umstandes, dass aufgrund der Verschiedenheit der Anwendbarkeit des Rechts im öffentlichen und privaten Bereich sich auch verschiedene Anknüpfungsmethoden als notwendig erweisen können. Folgende Ueberlegungen waren für die Wahl der Einheit von Jus und Forum massgebend:

- Mit einer getrennten Anknüpfung von Jus und Forum ist keineswegs sichergestellt, dass nach den Auseinandersetzungen um die Zuständigkeit auch wirklich das angemessenste bzw. kompetenteste der konkurrierenden Rechte zur Anwendung kommt und die materielle Gerechtigkeit am besten verwirklicht wird.²⁵
- Die durch die Wahl des ersteren Prinzips (Auseinanderklaffen von Jus und Forum) geschaffenen komplexen Verhältnisse helfen dem Betroffenen wenig, sein Persönlichkeitsrecht auf wirkungsvolle Weise durchzusetzen;²⁶ im Gegenteil, das Risiko von Rück- und Weiterverweisungen kann das Datensubjekt so belasten, dass dieses letztlich dazu kommen könnte, auf die Geltendmachung seiner Individualrechte überhaupt zu verzichten.
- Schliesslich sollte bei einem internationalen Tatbestand mit der Klärung des anwendbaren Rechts und der Zuständigkeit auch die Rechtssicherheit verwirklicht werden; dieses Postulat ist mit dem Prinzip, dass aus der Bezeichnung des anwendbaren Rechts auch die Zuständigkeit folgt (und umgekehrt) weitgehend erfüllt.

c) Mögliche Anknüpfungspunkte

aa) Anknüpfung am Wohnsitz des Datensubjektes

Dieser Anknüpfungspunkt liegt vom Zweckgedanken des Datenschutzes aus betrachtet am nächsten, weil ja das Datensubjekt und sein Persönlichkeitsrecht den Kern des Datenschutzes darstellen. Die Anknüpfung des anwendbaren Rechts und der zuständigen Be-

25 KELLER, S. 36f.

26 Gl.M. Rapport BISCHOFF, N 3-5.

hörde würden sich demnach nach dem Wohnsitz oder dem gewöhnlichen Aufenthaltsort ²⁷ der von der Datenbearbeitung betroffenen Person richten.

aaa) Vorteile

- Der aus einer solchen Anknüpfung resultierende Vorteil ist evident: Der Betroffene kann in allen Fällen sein Wohnsitzrecht auf Verletzungen seiner persönlichen Verhältnisse zur Anwendung bringen. Der dem Datensubjekt zukommende Schutz ist optimal, da die zuständigen Gerichte auch die territorialen und lokalen Gegebenheiten berücksichtigen können und der Betroffene nur auf das Datenschutzrecht seines Wohnsitz- bzw. Aufenthaltsstaates abstellen muss.
- Ein weiteres positiver Punkt ergibt sich aus der Vermeidung von sog. "small data havens": Durch die Anknüpfung am Wohnsitz des Datensubjektes ist es der datenverarbeitenden Stelle unmöglich, Abweichungen in der Regelungsintensität verschiedener Ordnungen gezielt auszunutzen und von einer liberaleren Gesetzgebung zu profitieren, da der Betroffene jederzeit die Möglichkeit hat, sein nationales und u.U. restriktives Gesetz auf einen Tatbestand zur Anwendung zu bringen. ²⁸

27 Vgl. Rapport BISCHOFF, N 3-5.

28 Die Anwendung des nationalen Rechts darf aber unter keinen Umständen dazu führen, dass - infolge fehlender Differenzierung und Relativierung des Anknüpfungspunktes - sich Fälle ereignen, die zu einer Sanktion bzw. Massnahme führen, obwohl die entsprechende Verarbeitungsart am Ort der Vornahme nach dem dort geltenden Recht keinen Gesetzesbruch darstellt. Ein solches Resultat wäre unerträglich, da der Datenverarbeiter sich bei gesetzeskonformem Verhalten darauf verlassen können muss, nicht zur Verantwortung gezogen zu werden. Bei der Ausgestaltung einer Anknüpfung am Wohnsitz des Datensubjektes wird deshalb besonders darauf zu achten sein, dass die Rechtssicherheit nicht durch solche Inkompatibilitäten gefährdet wird.

29 Diese Vielzahl ist nur theoretisch, da die Konvention einen geschlossenen Kreis von Mitgliedern bildet und somit nur das Recht von Mitgliedstaaten zur Anwendung kommen kann.

bbb) Nachteile

Die aus einer solchen Anknüpfung sich ergebenden Nachteile dringen z.T. schon bei der Argumentation der Vorteile durch:

- Durch diese Anknüpfungsart kann eine verantwortliche Stelle, eine Datensammlung oder ein Datenverarbeitungsvorgang gleichzeitig einer Vielzahl ²⁹ von Gesetzen und zuständigen Behörden unterworfen sein, die sich je nach Art der Bearbeitungshandlung und der geographischen Streuung der im Datenverarbeitungsprozess erfassten Daten-subjekte verschieden zusammensetzen. ³⁰
- Die datenverarbeitende Stelle kann in eine Konfliktsituation geraten, die sich daraus ergibt, dass sie von einer ausländischen Behörde zur Verantwortung gezogen werden kann, obwohl sie nach dem Recht des Verarbeitungsortes gesetzeskonform gehandelt hatte, wenn nach dem Recht am Wohnsitz des Betroffenen der Tatbestand als rechtswidrig qualifiziert wird. Wie erwähnt, ³¹ sollten solche Inkompatibilitäten bei der Schaffung von Kollisionsnormen innerhalb einer Konvention ausgeschaltet werden.
- Ein weiterer Nachteil ergibt sich beim Vollzug von Entscheiden, die eine zuständige ausländische Behörde erlassen hat. Ein Vollzug der durch das ausländische Aufsichtsorgan bzw. Behörde getroffenen Entscheidung ist nicht praktikabel, weil dieser ausserhalb ihres territorialen Machtbereiches, ³² am Ort eines Verarbeitungsvorganges oder der Datensammlung durchgeführt werden müsste.

30 Ebenso Rapport BISCHOFF, N 7.

31 Vgl. oben, Anm. 28.

32 D.h. Rechtsbereich des zuständigen Organs.

- Eine grundsätzlich andere, neuartige Situation ergibt sich, wenn das Datensubjekt seinen Wohnsitz oder Aufenthaltsort nicht in einem der Vertragsstaaten hat.^{33 34} In diesem Fall wäre die Kollisionsnorm wegen des Prinzips der geschlossenen Konvention nicht anwendbar; nach der gewählten Anknüpfungsform könnte dem Datensubjekt aber auch nicht der Schutz des Staates zukommen, in dem die Verarbeitung erfolgt oder die verantwortliche Stelle sich befindet, weil damit praktisch mehrere Anknüpfungsbegriffe innerhalb des Konventionsbereiches gelten müssten, da die Verarbeitung von Daten über Subjekten aus Nicht-Mitgliedstaaten wegen der Gleichstellung von In- und Ausländern nicht ausgeschlossen werden kann. In diesem Falle hätte ein subsidiärer Anknüpfungspunkt einen Ausweg zu schaffen und das Recht eines Konventionsstaates zur Anwendung zu bringen.

ccc) Folgerung

Die mit einer Anknüpfung am Wohnsitz bzw. Aufenthaltsort des Datensubjektes verbundenen Vor- und Nachteile bewirken eine einseitige Zuweisung von Vorteilen zugunsten des Datensubjektes und von Nachteilen zu Lasten des verantwortlichen Bearbeiters. Während dem Betroffenen eine optimale Rechtsstellung eingeräumt wird, erfährt der Datenverarbeiter eine Beschränkung innerhalb seines Handlungsraumes von legalen Datenverarbeitungsaktivitäten. Das Spannungsverhältnis zwischen rechtmässigem Verhalten am Ort der Verarbeitung und potentieller Verletzung nach dem Recht des Betroffenen ist für die datenverarbeitende Stelle absolut unerträglich und bedarf eines Ausgleiches der Rechtspositionen und der legitimen Interessen auf Seiten des Betrof-

33 Falls man das Prinzip der Gleichstellung und Gleichbehandlung von In- und Ausländern, unabhängig von ihrem Wohnsitz, einer Konvention zugrundelegt, beschränkt sich der Schutz analog zu Art. 1 EMRK nur auf die in den Vertragsstaaten wohnhaften bzw. sich aufhaltenden Personen.

34 Rapport BISCHOFF, N 9.

fenen und des Verarbeiters. In ihrer unrelativierten, reinen Anknüpfungsform scheint diese Lösung konfliktbeladen und nicht tauglich zur Lösung von Gesetzeskollisionen.

bb) Anknüpfung am Ort der Verarbeitungshandlung, d.h. am Ort, wo der Verarbeitungsvorgang stattfindet

Mit der Festlegung des Ortes der Verarbeitungshandlung hat auch eine Begriffsbestimmung zu erfolgen: Unter "Verarbeitungshandlung" ist jede Art der Verarbeitung von Daten zu verstehen, sei es dass diese speziell initialisiert wird oder Teil einer Kette von Verarbeitungsschritten darstellt. In diese Kategorie fallen ebenfalls die Handlungen, die notwendig sind, damit mittels automatisierter Einrichtungen auf Datenbanken zugegriffen werden kann.

Die Anknüpfung richtet sich hier nach dem Recht und Gerichtsstand desjenigen Ortes, an dem die Datenverarbeitung stattfindet und sich eine tatsächliche Rechtsverletzungshandlung auch ereignet; er verkörpert somit den klassischen Anknüpfungsgrundsatz der "lex loci delicti commissi", wie er im Rahmen des auf die Persönlichkeitsrechtsverletzungen anwendbaren Deliktstatuts vorgesehen ist.³⁵

aaa) Vorteile

- Die Anknüpfung am Ort des Verarbeitungsvorganges gibt jeder datenverarbeitenden Stelle die Möglichkeit, die Rechtmässigkeit bzw. Gesetzeswidrigkeit ihrer Handlungen aufgrund des am Verarbeitungsort geltenden Rechts selbst zu prüfen und zu beurteilen. Da die Verarbeitungshandlung ausschlaggebend für die Wahl des Forums und des anwendbaren Rechts ist, hat sich der Datenverarbeiter somit stets nur an sein einheimisches Recht zu halten und muss bei dessen gesetzeskonformer Handhabung keine nachteiligen Rechtsfolgen befürchten. Dies ist ein Umstand, der die Rechtssicherheit für alle datenverarbeitenden Stellen wesentlich erhöht.

35 VISCHER, S. 560.

- Der Vollzug von Entscheidungen und Massnahmen nach erfolgter Gesetzesverletzung lässt sich einfach durchführen, da die Behörde am Ort der Verarbeitung, d.h. dort, wo die Verletzung entstanden ist, direkt korrigierend und sanktionierend eingreifen kann. Der Vollzug erweist sich als perfekt, da eine territoriale Beziehung zwischen Vollstrecker und Verpflichtetem gegeben ist.

bbb) Nachteile

- Als negativ erweist sich die Anknüpfung am Ort der Verarbeitung zur Klärung der Frage des anwendbaren Rechts bei transnationalen Datenflüssen, vor allem bei Datenverarbeitungsnetzen und integrierten Systemen mit Verarbeitungskapazität in verschiedenen Ländern, da oft nicht feststellbar ist, wo der Verletzungsvorgang stattgefunden hat, weil ein internationales Datenverbundsystem für eine optimale Rechnerauslastung für spezielle Verarbeitungsschritte ausländische Hard- und Software für spezielle Verarbeitungsschritte benutzt wird. Aufgrund der komplexen Verknüpfung und des schnellen Ablaufs der Verarbeitungsvorgänge mit gleichzeitiger Uebermittlung der Daten ins Ausland ist nicht immer eine eindeutige Identifizierung des Verletzungsortes möglich, so dass hier gerade die Tatsache des grenzüberschreitenden Verarbeitungsvorganges der Klärung des Anknüpfungsortes Schwierigkeiten bereitet.
- Die Ausnutzung ausländischer Verarbeitungskapazität kann ausserdem dazu führen, dass an mehreren Orten rechtsverletzende Verarbeitungsschritte stattfinden, so dass neben dem Problem der Identifikation des Verletzungsortes noch das Problem konkurrierender Rechte und Gerichtsstände auftaucht. Da dem Datensubjekt aber nicht zugemutet werden kann, seine Rechte an allen Orten der Verletzungshandlungen geltend zu machen, müsste eine Zerlegung der Arbeitsschritte vollzogen werden und vorfrageweise eine Abklärung stattfinden, welcher der Verletzungsvorgängen der wesentlichste ist und für die Anknüpfung von Gerichtsstand und anwendbarem Recht konstitutiv wirkt. Daraus wird auch deutlich, dass ein unterschiedlicher Geltungsbereich des nationalen Rechts für die Abklärung des anwendbaren Rechts u.U. schwerwiegende Auswirkungen haben kann. In Staaten, die

nur die automatisiert verarbeiteten Daten schützen, wird eine manuelle Verarbeitungshandlung nie als rechtswidrig zu qualifizieren sein, obwohl sie nach dem Recht des Betroffenen - dessen Wohnsitzrecht auch die manuell verarbeiteten Daten schützt - als rechtswidrig zu beurteilen ist. Abgesehen davon, dass bei einem sich über mehrere Staaten erstreckenden Verarbeitungsprozess bestimmte Territorien für Umgehungshandlungen ausgenutzt werden können, veranschaulicht dieses Beispiel, dass diese Anknüpfungsmethode wegen der Ungleichheit der Geltungsbereiche zu materiell ungerechten Lösungen führen kann.

- Eine verantwortliche Stelle, die ein über mehrere Mitgliedstaaten sich erstreckendes Datennetz betreibt, würde sich bei einer Anknüpfung Ort des Verletzungsvorganges, unter strafrechtlichen Aspekten im Spannungsfeld mehrerer Strafsysteme zu verantworten haben, falls die strafrechtliche Handlung an mehreren Orten erfolgt ist. Der strafrechtliche Aspekt hebt sich insofern ab, als eine nach entsprechendem nationalem Recht erfolgte Erfüllung eines Straftatbestandes zwingend die Anwendung dieses Rechts erfordert.
- Da die Verarbeitung bei integrierten Datennetzen auch ausserhalb der Konventionsstaaten erfolgen kann, würde eine Verletzungshandlung in einem Drittstaat die Unanwendbarkeit der Kollisionsnorm bedeuten, m.a.W. der Verletzungsvorgang könnte nicht nach Konventionsrecht bzw. nach dem Recht eines Vertragsstaates sanktioniert werden.

ccc) Folgerung

Auch hier erweisen sich die mehreren möglichen Orte einer Verletzungshandlung als nachteiliger Faktor für eine Anknüpfung. Dem Betroffenen stellt sich die Vielzahl möglicher Orte der Anknüpfung insofern schwer lösbare Probleme, als er einerseits beurteilen und wissen muss, wo die betreffenden Handlungen bzw. Verarbeitungsschritte vollzogen wurden. Andererseits muss er nach der Identifizierung dieser Orte auch abklären, ob sie nach dem dort geltenden Recht überhaupt eine Rechtsverletzung oder ein Delikt darstellen. Mit der Klärung dieser Fragen aber wird das Datensubjekt bei einem Lastverbund, d.h. der Koppelung von Rechen- und Verarbeitungskapazität, eindeutig überfordert sein.

Auch für die datenverarbeitenden, verantwortlichen Stellen, die integrierte Datennetze betreiben, ist die Anknüpfung nach dem Deliktstatut wenig geeignet, da auch hier positive Gesetzeskonflikte nicht auszuschliessen sind: In der Vermeidung solcher Gesetzeskonflikte besteht aber der Sinn der Schaffung von Kollisionsnormen.

cc) Anknüpfung am Ort der Benutzungshandlung bzw. am Ort jedes Benützers der Daten

Hier ist vorerst der Begriff der Benutzungshandlung zu definieren und von der Verarbeitungshandlung abzugrenzen:

Die Verarbeitungshandlung geht i.d.R. einer Benutzungshandlung vor, d.h. während der Verarbeitungshandlung erfahren die Daten in ihrem Bestand durch die Verarbeitung eine Aenderung, Umformung, Ergänzung, Auswahl, Verknüpfung, Speicherung, Vernichtung usw.; anschliessend an diese Verarbeitungsvorgänge folgt die Benutzungshandlung, z.B. durch eine Verfügung, Entscheidung, Willensäusserung oder andere Handlung, die aufgrund der bearbeiteten Daten vorgenommen wird. Durch die Benutzung der Daten wird dem Datensubjekt aber normalerweise die Persönlichkeitsverletzung erst bekannt und manifest. Die Persönlichkeitsverletzung kann nun einerseits schon mit dem Abschluss der Verarbeitungshandlungen existieren (d.h. vor Vornahme einer Benutzungshandlung), andererseits aber auch erst durch die Ausübung der Benutzungshandlung verursacht werden, z.B. bei Verwertung der erlangten personenbezogenen Informationen.

Hinsichtlich der Benutzungshandlung und der Anknüpfung ist entscheidend, welcher Personenkreis in der Definition mit dem Attribut 'Benutzer' versehen wird. So kann z.B. eine Stelle, die mittels eines Terminals auf eine Datensammlung im Ausland zugreift, selbst aber kein Verfügungsrecht über die Daten hat, als Benutzer deklariert werden; es ist aber auch denkbar, dass sie von einem nationalen Gesetz als verantwortliche Stelle bezeichnet wird.³⁶ Bearbeiter und Benützer können aber auch zusammenfallen und werden in der Regel auch identisch sein, so dass der Benützer vermutlich immer nur der reine Empfänger ist.

aaa) Vorteile

- Die Anknüpfung am Ort des Benutzers wirkt sich positiv aus, wenn das Benutzungsland mit dem Wohnsitzstaat des Datensubjektes identisch ist. Diesfalls ist es für den Benutzer der Daten einfach, sich zu orientieren, wie eine persönlichkeitsverletzende Verwendung der Daten vermieden werden kann. Eignet sich eine Persönlichkeitsverletzung, ist es für das in seinen Rechten beeinträchtigte Datensubjekt und die zuständigen Behörden leicht, gegen die Verletzung vorzugehen und die entsprechenden Massnahmen zu vollstrecken.
- Bei einer Persönlichkeitsverletzung durch den Benutzer ergibt sich für das Datensubjekt nur ein Anknüpfungspunkt. Befindet er sich im gleichen Land, wie das Datensubjekt, stellen sich weiter keine Probleme, da sich der internationale Tatbestand mit der Anwendung eines Rechtes, dem Recht des Datensubjektes und dem des Benutzer lösen lässt. Es resultiert mit diesem Anknüpfungspunkt unter den gegebenen Voraussetzungen eine Lösung auf nationaler, innerstaatlicher Ebene.

bbb) Nachteile

- Die nachteilige Seite dieses Anknüpfungspunktes kommt dann zum Vorschein, wenn der Staat, in dem die Daten benutzt werden, nicht mit dem Wohnsitzland des Betroffenen zusammenfällt. Das Datensubjekt muss sich bei der Behandlung seiner Ansprüche nach den Vorschriften eines andern Rechtskreises richten, was u.U. zu stossenden Ergebnissen führen kann, vor allem weil der Datenschutz in seiner materiellrechtlichen Ausprägung territoriumsbezogen und vom nationalen Kontext der Rechtsordnung insgesamt abhängig ist.³⁷

36 Hier erweist sich, dass international einheitliche Begriffsbestimmungen und Definitionen zur Lösung des Kollisionsproblems im Datenschutz einen wesentlichen Beitrag leisten.

37 Z.B. Schweden: Seit 1766 ist das Prinzip des freien Zugangs von Individuen zu öffentlichen Daten der Behörden gesetzlich verankert (vgl. FREESE, Data Flow, S. 17; GASSMANN/PIPE, OECD Informatics Studies 10, S. 16).

- Es kann möglich sein, dass sich aus einer vom Benutzer begangenen Verletzungshandlung negative Auswirkungen auf die bearbeitenden Stellen im Ausland ergeben, z.B. durch den Vollzug eines Entscheides wie die Löschung bestimmter Datenbestände.
- Mögliche unterschiedliche nationale Definitionen der Begriffe von Benutzer und verantwortlicher Stelle können zu weiteren Inkompatibilitäten und Kollisionen führen. Die Anknüpfung an den Begriff der Benutzung würde daher eine internationale Vorschrift voraussetzen, die eine einheitliche Abgrenzung zwischen Benutzer und verantwortlicher Stelle vornehmen müsste.
- Bei der Anknüpfung an das Recht des Benützungsortes können sich für die verarbeitende Stelle weitere Nachteile ergeben: Der Staat, in dem die Benutzung vollzogen wird, wäre imstande, die Personen, die von seinem Territorium aus Daten im Ausland benützen wollen (z.B. mittels Terminal), zu hindern, die Benutzungshandlung durchzuführen. Er wird dazu neigen, nicht nur bezüglich der Benutzung Vorschriften zu erlassen, sondern auch hinsichtlich der zulässigen Verarbeitungsart, so dass der ausländische Datenbankhalter oder ein Rechenzentrum seine Leistungen an Benützer im anderen Staat nur anbieten kann, wenn er sich dem Recht und der Zuständigkeit des Terminalstaates unterwirft. Für die verantwortliche Stelle der Datenbank oder eines Service-Centers kann dies u.U. eine erhebliche Belastung darstellen, da sie sich stets im Spannungsfeld mehrerer Rechtsordnungen - mitsamt ihren zwingenden Normen - befindet und Unvereinbarkeiten mit einheimischen Bestimmungen denkbar sind.

ccc) Folgerung

Da die Benutzungshandlung nur einen Teilaspekt (Verwendung, Nutzung der Daten) möglicher Persönlichkeitsverletzungen im Zusammenhang mit der Verarbeitung von Informationen darstellt, ist mit diesem Anknüpfungspunkt das Problem nicht abschliessend gelöst. Diese Art der Anknüpfung erweist sich nur dort als zweckmässig, wo Benutzer und Datensubjekt sich unter gleicher Rechtshoheit befinden. Für Persönlichkeitsverletzungen, die aus gesetzeswidriger Verarbeitung resultieren, wäre ein anderer Anknüpfungspunkt notwendig.

dd) Anknüpfung am Wohnort oder Geschäftssitz der verantwortlichen Stelle

Allgemein kann als verantwortliche Stelle, diejenige natürliche oder juristische Person bezeichnet werden, die die zu verarbeitenden Daten, ihre Erhebung, Speicherung, die Arten und Abläufe sowie den Zweck der Bearbeitung bestimmt oder beaufsichtigt. Die exakte Begriffsumschreibung dieser Stelle bleibt den nationalen Rechten (oder einer internationalen Vereinbarung)³⁸ überlassen.

Der Anknüpfungsort richtet sich nach dem Wohn- oder Geschäftssitz der verantwortlichen Stelle: Sie untersteht damit grundsätzlich der Behörde ihres Sitzstaates und ist überdies nicht nur für die auf ihrem nationalen Territorium stattfindenden Verarbeitungsvorgänge nach dem Datenschutzrecht des Sitzstaates zu beurteilen, sondern auch für die sich im internationalen Bereich abspielende Datenverarbeitung. Daraus folgt, dass die verantwortliche Stelle bei Persönlichkeitsrechts- und Gesetzesverletzungen auf internationaler Ebene immer nach dem Recht ihres Wohn- bzw. Geschäftssitzstaates und vor den einheimischen Behörden zur Verantwortung gezogen werden kann.

Die Bezeichnung des Aufenthaltsortes einer verantwortlichen Stelle als subsidiärer Anknüpfungspunkt, ist angesichts der mit diesem Begriff verbundenen Variabilität der Ortsbestimmung in mehreren Staaten, woraus eine Unterstellung unter wechselnde Rechtsordnungen folgen würde, im Interesse der Rechtssicherheit abzulehnen.

38 In den verschiedenen Datenschutzgesetzen heisst diese verantwortliche Stelle z.B. "speichernde Stelle" (BRD), "Auftraggeber" (AU); ausserdem existieren dafür die Bezeichnung "maître de fichier" (KE, RL) oder "controller of the file", Registerführer, Datenverarbeiter, Datenbankführer etc.

aaa) Vorteile

- Die Anknüpfung am Wohn- bzw. Geschäftssitz bringt der verantwortlichen Stelle den Vorteil, dass an demjenigen Punkt angesetzt wird, wo die Verantwortung für die gesamte Datenverarbeitung konzentriert ist; m.a.W. es kann diejenige Stelle zur zivilrechtlichen, verwaltungsrechtlichen oder strafrechtlichen Verantwortung gezogen werden, die den Entscheid über die zu beurteilenden Verarbeitungsvorgänge gefällt hat, so dass bei der Klärung der rechtlichen Verantwortung keine Spannungsverhältnisse zwischen verschiedenen Rechtsordnungen mehr auftreten können.
- Diese Anknüpfungsart erweist sich für die verantwortliche Stelle auch deshalb als optimal, weil sie nach dem ihr bekannten Recht des Geschäftssitz- oder Wohnsitzstaates beurteilt wird. Damit fällt es dem Datenverarbeiter leicht, bei internationalen Tatbeständen das anwendbare Recht und die damit verbundenen Rechtsfolgen für die Verarbeitung vorherzusehen. Dieser Anknüpfungspunkt bringt deshalb keine Behinderung der normalen DV-Tätigkeit aus rechtlichen Gründen, da die Rechtssicherheit auf Seiten der verantwortlichen Stelle gewährleistet ist.
- Ein dritter positiver Punkt dieses Anknüpfungsortes wird bei der Vollstreckung und Durchsetzung von Behördenentscheidungen offenbar: Durch die Einheit von Jus und Forum kann die Anerkennung und Vollstreckung des Urteils nicht mit dem Vorbehalt des "ordre public" zu Fall gebracht werden, da die lokale Behörde ihr einheimisches Recht anzuwenden hat und der Vorbehalt des "ordre public" logischerweise nicht gegenüber der eigenen Rechtsordnung zur Anwendung kommen kann. Der Vollzug eines Urteils ist gewährleistet, weil der Vollstreckungsort und der Sitz des Verantwortlichen nicht auseinanderfallen. Diese Anknüpfung bietet Gewähr, dass diejenigen Datenverarbeiter, die tatsächlich eine Verbesserung der Datenverarbeitungsabläufe oder eine Beseitigung von Missständen bewirken können, auch wirklich zu deren Ausführung angehalten oder gezwungen werden können. Die Durchführung von Massnahmen ist somit von den Behörden des gleichen Landes überprüfbar und erzwingbar, die den Sachentscheid gefällt haben.

bbb) Nachteile

- Auch mit dieser Anknüpfungsart ergeben sich mehrere örtliche Zuständigkeiten: Bei einem Netzverbund oder einem integrierten Datenverarbeitungssystem, bei dem zur Bearbeitung der Daten eine Kopplung der Rechen- und Verarbeitungskapazität von ausländischen Systemen vorgenommen wird,³⁹ können die in verschiedenen Ländern befindlichen DV-Anlagen mehreren verantwortlichen Stellen⁴⁰ unterstehen. Wie vorgehend⁴¹ ausgeführt, sind bei diesen integrierten Systemen und beim Lastverbund der Ort und Urheber einer Verletzung nicht immer eindeutig festzustellen, so dass dem Betroffenen nicht klar ist, welche der verantwortlichen Stellen er ins Recht zu fassen hat. Eine zusätzliche vorfrageweise Abklärung, an welchem Ort die tatsächliche Verletzungshandlung erfolgt ist, sollte dem bei dieser Art der Anknüpfung ohnehin schon in einer unvorteilhaften Ausgangslage befindlichen Datensubjekt nicht zusätzlich aufgebürdet werden.⁴² In einem Entwurf für ein schweizerisches Datenschutzgesetz wäre daher für Datenbanken und Netzwerken die Bezeichnung einer obligatorischen Stelle zu fordern, die nach aussen die Verantwortlichkeit für das Netzwerk bzw. den Verbund und nach innen die Durchsetzung des Datenschutzes übernimmt.
- Ergeben sich mehrere Anknüpfungspunkte, taucht ein neues Problem auf, falls die von einem Datensubjekt angestrebte Klage sich nur auf eine verantwortliche Stelle bezieht, an der Rechtsverletzung aber noch weitere Verarbeiter und Personen in andern Staaten beteiligt sind. In diesem Falle könnte eine solidarische Haftung unter den Beteiligten in den Mitgliedstaaten das zivilrechtliche Ver-

39 Lastverbund, vgl. vorne, S. 285, Anm. 5.

40 Z.B. SWIFT, die ausführenden DV-Stellen befinden sich in Holland, Belgien und USA; die verantwortlichen Stellen sind hier m.E. bei den einzelnen SWIFT-Banken (vgl. vorne, S. 64 und bes. 69f.). IBM-SWITCH, Rechenzentren sind in Cosham und Uithoorn, (vorne, S. 85f.).

41 Vgl. vorne, S. 310ff.

42 Vgl. nachfolgende nachteilige Punkte.

antwortlichkeitsproblem lösen; m.E. ist auch eine Solidarität hinsichtlich Vollzug von Auflagen und Massnahmen der Datenschutzbehörden denkbar. Bei der strafrechtlichen Verantwortlichkeit ergeben sich allerdings wegen des individuellen, poenalen Charakters der Strafe und ihrer Anwendbarkeit auf eine bestimmte Person Probleme.⁴³ Ausserdem müssen bei dieser Konstellation die Behörden des Sitzstaates der mitverantwortlichen Stelle den aufgrund des zuständigen, anwendbaren Rechts im Ausland gefällten Entscheid vollstrecken.⁴⁴ Dies würde die örtlich einheitliche Trias von Rechts-
hoheit, anwendbarem Recht und Vollstreckungshoheit wieder spalten. Man könnte hier (z.B. mittels Konvention) eine ex lege "Vereinigung" der Verfahren gegen die verantwortlichen bzw. mitverantwortlichen Stellen in verschiedenen Rechtsbereichen postulieren. Keine Anknüpfungsprobleme sollten entstehen, wenn für ein Daten-
netz bzw. ein Systemverbund nur eine verantwortliche Stelle mit einem Sitz in einem Mitgliedstaat vorhanden ist.

- Die Anknüpfung am Geschäfts- bzw. Wohnsitz der verantwortlichen Stelle birgt die Gefahr der Bildung von "small data havens" oder sog. "Convention havens".⁴⁵ Konventionsländer mit einer trotz gemeinsamen Minimalstandard nach oben oder unten abweichenden Regeldichte können zum bevorzugten Ort beim Errichten von Geschäfts- oder Wohnsitzen verantwortlicher Stellen werden. Favorisiert wären vermutlich diejenigen Mitgliedstaaten, deren Datenschutzrecht u.a. weniger einschneidende Sanktionsbestimmungen und Verantwortlichkeitsnormen aufweisen; das Ausnützen von unterschiedlichen Rechtsordnungen ist aber ein erlaubtes Mittel (vgl. Steuergesetze).
- Hauptproblem der Anknüpfung am Ort der verantwortlichen Stelle bleibt die Benachteiligung des Datensubjektes, die sich im mehrfachen Weise manifestiert:

43 Rapport BISCHOFF, N 9.

44 Id., a.a.O.

45 Vgl. vorne, S. 44f.

46 STARCK, ZBJV 114 (1978), S. 361.

Es ist dem geschädigten Betroffenen, ebenso wenig wie im Falle der Produkthaftungspflicht,⁴⁶ zumutbar, eine verantwortliche Stelle an einem weit abliegenden Gerichtsstand einzuklagen und dort sein Recht durchzusetzen, weil dies kompliziert, teuer und risikoreich sein kann, so dass viele Datensubjekte aus diesen Gründen von der Wahrnehmung ihrer Rechte zurückschrecken könnten.⁴⁷ Auch hier liessen sich Aushilfen denken wie z.B. die Vorschrift, dass verantwortliche Stellen überall dort, wo sie DV betreiben, einen Zustellbevollmächtigten haben, an welchen streitige und nicht streitige Ansprüche zu adressieren sind.

- Obwohl der "noyau dur" eine gewisse Harmonisierung anstrebt, ist ein von Land zu Land unterschiedlicher Schutzgrad nicht zu vermeiden, weil die nationalen Gesetze divergierende Schutzbereiche, Geltungsbereiche und Anwendungsbereiche (i.e.S.) definiert haben; besonders im öffentlichen Bereich kann eine unterschiedliche rechtliche Ausgestaltung für ein Datensubjekt, das sich einem fremden Recht unterwerfen muss, erhebliche Probleme bringen.
- Hat die verantwortliche Stelle ihren Wohnsitz nicht in einem der Konventionsländer, sondern in einem Drittstaat, ist, des Prinzips der geschlossenen Konvention wegen, weder das Recht noch die Behörde eines Konventionslandes zuständig, so dass eine rechtliche "Patt-Situation" auftreten kann.

Für solche Fälle müssen die nationalen Datenschutzgesetze eine Lösung vorsehen, wenigstens für den Fall, wo sich Verletzungshandlungen, die von einer Stelle in einem Nicht-Konventionsland ausgehen, im nationalen Territorium auswirken.

ccc) Folgerung

Dank dem Prinzip der gleichartigen Anknüpfung von Rechtsprechungshoheit und anwendbarem Recht erhält man mit der Anknüpfung am Sitz der verantwortlichen Stelle eine materielle wie zuständigkeitsmässige Uebereinstimmung der Verantwortung für Entscheidungen⁴⁸

47 Hier werden ausserdem noch Sprachprobleme hemmend wirken.

48 Der verantwortlichen Stelle.

über Verarbeitungsvorgänge auf Seiten des Datenverarbeiters und der Zuständigkeit der gerichtlichen und administrativen Behörden (für Urteile und Massnahmen) und deren Vollstreckung. Ein derartiger Anknüpfungspunkt bietet Gewähr für die Effizienz der Sanktionen und Anordnungen, so dass er sich hinsichtlich der Vollstreckung und Durchsetzung auf internationaler Ebene als praktikabel erweist. Die extrem ungünstige Stellung des Betroffenen hat in diesem Modell aber einen hemmenden Einfluss auf die Verwirklichung der Individualrechte, vor allem wegen der nationalen materiell- und formellrechtlichen Verschiedenheit der Rechtsordnungen.

Diese Kollisionsnorm würde sich als anwendbar erweisen, wenn in allen Mitgliedstaaten ein einheitliches, d.h. harmonisiertes und somit weitgehend uniformes Datenschutzrecht existieren würde, weil dann die Wahrnehmung der für den Betroffenen geltenden Rechte im Ausland nicht erschwert wäre.

B. Schlussfolgerung

Es ist nicht möglich, einen der aufgeführten Anknüpfungspunkte für die Lösung des Problems der Gesetzeskollisionen als ideal zu bezeichnen, da ein jeder gewichtige Vor- und Nachteile aufzuweisen hat.

Entscheidend bei der Festsetzung eines solchen Anknüpfungspunktes scheint mir der Zweckgedanke des Datenschutzes, der im nationalen wie internationalen Bereich den Schutz der Persönlichkeit aber auch die Informationsfreiheit anstrebt. Dies bedeutet, dass die Wahl auf eine Form der Anknüpfung fallen sollte, die dem Datensubjekt eine günstige Ausgangslage für die Geltendmachung seiner Individualrechte verschafft; umgekehrt könnte das andere Extrem einer evidenten Schlechterstellung des Datenverarbeiters bzw. der verantwortlichen Stelle einen hindernden Einfluss auf die Verarbeitung personenbezogener Daten im transnationalen Bereich ausüben.

Für den öffentlichen Bereich sind wiederum andere Massstäbe gültig, da der Austausch der Daten nur aufgrund einer gesetzlichen Bestimmung (völkerrechtlicher Vertrag) vollzogen werden kann und die Bearbeitung selbst nach dem Legalitätsprinzip erfolgen muss. Kommt es trotzdem zu einer Fehlbehandlung von Daten im Ausland, ist nur das öffentliche Recht jenes Staates anwendbar, dessen Behörde die Ver-

letzung des Persönlichkeitsrechts begangen hat. Das Prinzip der Gesetzmässigkeit der Verwaltung steht der Heranziehung eines ausländischen öffentlichen Rechtes entgegen, so dass die Behörde bei einer Anknüpfung am Wohnsitz des Betroffenen von Gesetzes wegen nicht das am ausländischen Wohnsitz eines Betroffenen geltende Recht anwenden kann.⁴⁹

Die anstehenden Fragen bedürfen zur Lösung und Bestimmung des zuständigen Jus und Forum einer grundlegenden Analyse und Diskussion durch Spezialisten des internationalen Rechts, denen hier nicht vorgegriffen werden soll.

C. Beschränkung des Anwendungsbereiches durch ein Konventionsmitglied

Der Rapport BISCHOFF⁵⁰ erwähnt noch den speziellen, von der Konvention des Europarates⁵¹ eingeräumten Fall der Ausklammerung⁵² von Daten aus dem Anwendungsbereich der Konvention durch einen Mitgliedstaat. Die Ausklammerung und Beschränkung des Anwendungsbereiches stellt besonders heikle Probleme,⁵³ weil die Gleichwertigkeit der Datenschutzrechte zwischen den Vertragsstaaten in Frage gestellt werden kann. Im Falle einer Beschränkung des Anwendungsbereiches ist dem betreffenden Konventionsstaat die Zuständigkeit sowie die Kompetenz zur Beurteilung der Rechtsfrage abzusprechen und insofern wie ein Drittstaat (Nicht-Konventionsstaat) zu behandeln.⁵⁴

3. Kollisionsprobleme im Verhältnis von Konventionsstaaten zu Drittstaaten

A. Begriff der Drittstaaten

Ausgangspunkt ist die Form einer sog. "geschlossenen Konvention", die sich aus den Mitgliedern eines völkerrechtlichen Vertrages zusammensetzt.

⁴⁹ Theorie des Verwaltungsaktes oder "act of state doctrine".

⁵⁰ Vgl. Rapport BISCHOFF, N 20 und 16.

⁵¹ Art. 3 Abs. 2 lit. a,b,c und 11 KE, vorne, S. 249f. und 256f.

⁵² Z.B. Beschränkung auf den Schutz nur natürlicher Personen, nicht auch juristischer Personen.

Da gemäss dem Prinzip der geschlossenen Konvention bei einer Kollision immer nur das Recht oder die Behörde eines Vertragsstaates zur Lösung einer Rechtsfrage zuständig sein kann, sind Drittstaaten - aus der Sicht der Konventionsstaaten - all diejenigen Länder, die die Konvention nicht ratifiziert haben. Dabei bleibt unberücksichtigt, ob der Drittstaat innerhalb seines Rechtssystems über Datenschutzbestimmungen verfügt oder nicht.

B. Problem

Innerhalb der Konventionsstaaten soll der grenzüberschreitende Datenverkehr - entsprechend dem Zielprinzip des freien Informationsflusses - ohne behördliche, wirtschaftliche, rechtliche oder anders geartete Schranken frei vollzogen werden können. Dieser freie transnationale Datenstrom ist möglich, weil in den einzelnen Gesetzen der Vertragsstaaten ein ungefähres Gleichgewicht an Schutzwirkung verwirklicht ist.⁵⁵ Da aber diese Gleichwertigkeit nicht absolut sein kann, gibt es innerhalb der Konventionsstaaten Abweichungen vom Mittelwert des Schutzdispositivs nach oben und nach unten.⁵⁶ Auch die Regelung des grenzüberschreitenden Datenverkehrs in den nationalen Gesetzen der einzelnen Mitgliedstaaten können untereinander erhebliche Unterschiede aufweisen; diese Abweichungen treten aber immer dann - auch unter den Mitgliedstaaten - besonders klar zutage, wenn sich der transnationale Verkehr nicht auf Vertragsländer beschränkt, sondern auch auf Drittstaaten erstreckt, die nicht mehr den minimalen Schutzstandard gemäss der Konvention erfüllen, sei es, dass sie überhaupt keine datenschutzrechtlichen Normen in ihrer Rechtsordnung kennen oder ein Datenschutzgesetz zwar vorhanden ist, der betreffende Staat jedoch nicht der Konvention angehört.

53 Vgl. MEISTER, DS+DS, 1/80, S. 13.

54 Rapport BISCHOFF, N 20.

55 Zweck des "noyau dur".

56 Analog zu den data havens, deshalb die Bezeichnung "Convention havens", vgl. vorne, S. 44.

Abweichung nach oben: restriktive Datenschutzgesetzgebung: Abweichung nach unten: Schutz erfüllt nur die Minimalanforderungen des noyau dur und ist im übrigen sehr grobmaschig.

57 Vgl. Synopsis, vorne § 9, S. 133ff.

Hier stellt sich - angesichts der national differierenden Regelungen zum grenzüberschreitenden Datenverkehr - die Frage, wie innerhalb der Konventionsstaaten eine praktikable Lösung gefunden werden kann, die verhindert, dass ein Vertragsstaat mit einer "largen internationalen Regelungskomponente" zum "Ausflussrohr" personenbezogener Informationen aus dem Konventionsgebiet in das weniger "datenschutzbewusste" Ausland wird. Die Funktion eines Ausflussrohres zeigt sich darin, dass Datenverarbeiter, die nach nationalem Recht keine Exportgenehmigung in einen bestimmten Drittstaat erhalten würden, diese Schranke dadurch zu umgehen versuchen, dass sie die Daten in einen andern Konventionsstaat verlagern und sie von dort aus an den Drittstaat übermitteln, weil dieser andere Konventionsstaat weniger restriktive Exportbestimmungen kennt.

Sollte ein solches "Datenleck" innerhalb eines Konventionsgebietes auftreten, würden vermutlich rasch neue Exportschranken durch die übrigen Konventionsstaaten aufgebaut, so dass unter den Vertragsstaaten eine Polarisierung und neue Gruppen entstehen könnten und für die Verwirklichung der Zielprojektion des freien Datenflusses neue Lösungen entwickelt werden müssten. Eine solche Entwicklung dient weder denjenigen Verarbeitern, die im Rahmen ihres Geschäftszweckes auf den grenzüberschreitenden Datenverkehr angewiesen sind, noch den Datensubjekten. Dieses konventionsinterne Problem bedarf m.E. einer möglichst einfachen und klaren Lösung: Eine solche ist aber nicht ohne materiellrechtliche Vorschrift auf Konventionsebene zu erreichen.

C. Lösungsmodell

Das hier dargestellte Lösungsmodell ist relativ einfach, bedingt aber eine Einschränkung der Entscheidungsfreiheit des nationalen Gesetzgebers hinsichtlich der Regelung des Wieder-Exportes von bereits in seinen Rechtsbereich übermittelten Daten.

Das Modell basiert auf dem Prinzip, dass nur personenbezogene Angaben eigenen Ursprungs aus einem Konventionsstaat in ein Drittland exportiert werden dürfen. Dies bedeutet m.a.W., dass unter den Konventionsstaaten ein grundsätzliches Verbot der Wiederausfuhr an Drittländer für all diejenigen Daten vereinbart würde, die an einen Kon-

ventionsstaat übermittelt oder übertragen wurden. Ein Konventionsstaat kann den Export nur freigeben, wenn es sich um eigene, im Inland beschaffte Daten handelt.

An dieser Stelle hat eine Bestimmung der Begriffe des "Ursprungslandes" und "originäre Daten" zu erfolgen: Die Eigenschaft des Ursprungslandes wird durch den erstmaligen Export ⁵⁸ eines Datums bestimmt, d.h. durch einen manuellen oder automatisierten Verarbeitungsvorgang, der bewirkt, dass das Datum den eigenen Rechtskreis verlässt, charakterisiert sich innerhalb des Konventionsgebietes ein Mitgliedstaat als "Ursprungsland".

"Originäre Daten" sind diejenigen Informationen, die innerhalb eines Konventionslandes durch direkte oder indirekte Angabe des Betroffenen manuell oder automationsunterstützt erfasst werden, d.h. die Herkunft der Daten bestimmt sich nach dem Ort bzw. dem Land des ersten manuellen oder automatisierten Verarbeitungsschrittes (z.B. Erfassung, Erhebung). ⁵⁹

Die Begriffe "originäre Daten" und "Ursprungsland" sind Korrelate, d.h. das Land der Entstehung eines originären Datums ist immer auch das Ursprungsland.

Das dargestellte Lösungsmodell, das auch als grundsätzliches Verbot des wiederholten Exportes bereits übermittelter Daten umschrieben werden kann, bewirkt für den Informationsverkehr mit Drittstaaten eine absolute Isolation Nicht-Ursprungsländer unter den Konventionsmitgliedern: Es können keine Leckstellen ausgenutzt werden, da die

58 Unter (erstmaligem) Export ist jeder Verarbeitungsvorgang manueller oder automatisierter Natur zu verstehen, der zur Folge hat, dass das Datum in einen andern Rechtskreis eintritt: Mit dem Einbezug manueller Verarbeitungsphasen soll den Fällen vorgebeugt werden, wo Daten manuell erfasst und hierauf unkontrolliert, d.h. ungeschützt (z.B. auf ausgefüllten Formularen oder Lochbelegen) ins Ausland zwecks nachfolgender Datenverarbeitung übermittelt werden.

59 Ähnliche Aufteilung bei GOTLIEB/DALFEN/KATZ, S. 236f.: "data gathering act and ... second act, i.e., the transmission of the information across the border to the data bank ...".

einzig zum Export befugte Stelle der Ursprungsstaat selbst ist, der auch das grösste Schutzinteresse an den innerhalb seines Gebietes entstandenen Daten bekunden wird.⁶⁰

Für konsolidierte Daten, die innerhalb eines Konventionsstaates erarbeitet werden, deren Einzelangaben aber aus verschiedenen Staaten stammen, ist kein Export an einen Drittstaat möglich, vielmehr müssen die Bearbeiter in den Drittstaaten direkt auf die entsprechenden Ursprungsstaaten zurückgehen, d.h. die konsolidierende Stelle im Drittstaat muss den Nachweis für den Schutz der personenbezogenen Informationen gegenüber jedem Ursprungsstaat leisten.^{61 62}

Der Grundgedanke und die Folge dieser Lösungsformel ist die Verlagerung des Kollisionsproblem es beim Datenverkehr mit Drittstaaten von der internationalen auf die nationale Ebene. Dadurch wird sichergestellt, dass allein dem Ursprungsstaat von Daten die Kompetenz zusteht, einen Export ins Ausland zu genehmigen oder zu untersagen; die Rechtsordnungen anderer Konventionsmitglieder können also nicht mehr dazu benützt werden, die Entscheidungen des bezüglich des Exportes

60 I.d.R. sind dies zum grössten Teil auch die Daten der im Gebiet eines Staates wohnhaften bzw. sich aufhaltenden Personen.

61 Bei multinationalen Firmen, die von allen Mitgliedsstaaten eine Exportgenehmigung in den bezeichneten Drittstaat besitzen, wäre eine Ausnahme denkbar.

62 Wenn der Grundsatz des Exportverbotes bereits ausgeführter Angaben an Drittstaaten durch ein anderes Konventionsland als der Ursprungsstaat in einer Ausnahmeregelung durchbrochen werden sollte, müssten andere Einschränkungen in Kauf genommen werden, die innerhalb eines Konventionsraumes gegenüber dem dargestellten Lösungsmodell (Ursprungsprinzip) beträchtliche Nachteile verursachen könnten. Würde z.B. von dieser Ausnahmeregelung Gebrauch gemacht, d.h. wenn über einen Vertragsstaat bereits exportierte Daten an einen Drittstaat übermittelt werden, liesse sich nicht vermeiden, dass der Ursprungsstaat bereits gegenüber dem Vertragsstaat Restriktionen und Genehmigungen anwendet im Hinblick darauf, dass dieser Vertragsstaat die Daten ohne weitere spezielle Genehmigung nach der Verarbeitung an den Drittstaat exportiert. Damit werden innerhalb des Konventionsbereiches neue Hindernisse für Datentransfers errichtet, die letztlich bei allen DV-Vorgängen eine Genehmigung rechtfertigen liessen, so dass der Grundsatz des freien Datenflusses zur Farce würde.

wirklich zuständigen Landes (Ursprungsstaat) zu unterlaufen oder zu vereiteln. Eine Transitformel nach dem Muster des Art. 12 Abs. 3 lit. b KE⁶³ wäre demnach hinfällig.

Mit einer solchen Regelung würde konventionsintern der freie Datenverkehr unterstützt; im Verhältnis zu Drittstaaten bliebe dagegen die Kompetenz zur Regelung des Exportes allein beim Ursprungsstaat, so dass für die Entscheidung auftretender Kollisionsprobleme die Zuständigkeit des nationalen Rechts gegeben ist und demnach jeder Ursprungsstaat nach seinen nationalen Regelungskriterien die Zulässigkeit bzw. Unzulässigkeit des Exportes beurteilen kann.

Zu einer optimalen Orientierung über die Herkunft eines Datums könnte die Einführung eines Landescodes und einer Registernummer als Exportvoraussetzung vorgesehen werden. Diese formale Vorschrift hat nun insofern einen weitreichenden Einfluss, als im Noyau nur oder über eine international rechtsetzende Norm die formellen Vorschriften zum Export modifiziert werden müssten und den freien Export von einem Eintrag in einem Datenverarbeitungsregister und der Ausstellung einer Registernummer abhängig machen sollten.⁶⁴ Die Registernummer der verantwortlichen Stelle wäre bei jedem Verarbeitungsschritt den Daten auf einem sog. "Datenindossament" beizufügen, so dass jede Weitergabe diese Datums durch eine lückenlose Kette solcher Herkunftshinweise dokumentiert wäre. Dadurch könnte im grenzüberschreitenden Datenverkehr genau festgestellt werden, wo die Daten ihren Ursprung haben und

63 Vgl. vorne, S. 260f.

64 Diese formelle Vorschrift ist in gewissen Ländern (z.B. Österreich) bereits verwirklicht, in andern wäre der Schritt dazu nur minimal, weil bereits der Eintrag in einem Datenverarbeitungsregister als Zulässigkeitsvoraussetzung für die Bearbeitung vorgesehen ist, so dass als Ergänzung nur noch die Erteilung einer Registernummer eingeführt werden müsste. Für Staaten, die eine Registrierung aller datenverarbeitenden Stellen ablehnen, wäre die Registrierung als Exportvoraussetzung zu konzipieren: Somit müssten nur die Stellen die einen grenzüberschreitenden Datenverkehr unterhalten, eine einmalige Registrierung vornehmen. Eine solche Vorschrift ist rein deklaratorischer Natur und stellt keine Behinderung oder Schranke für den freien transnationalen Datenfluss dar.

an welchen Stellen sie verarbeitet wurden. Die Registernummer würde dem Betroffenen helfen, die Verschiebungen seiner Daten a posteriori leichter zu verfolgen und dabei die für Verletzungen haftbaren Stellen zu identifizieren.

Die Frage des Datenimportes durch einen Konventionsstaat mit nachfolgendem Export lässt sich nach einem analogen Schema lösen, wobei zwei Fälle getrennt betrachtet werden müssen:

- Importiert ein Vertragsstaat Daten aus einem Drittstaat zur anschließenden Weiterverarbeitung in einem oder mehreren Konventionsstaaten, ohne dabei Verknüpfungen mit Daten aus dem Konventionsgebiet vorzunehmen, ist allein der Importstaat für die Zulässigkeit der Wiederausfuhr zuständig. Die Annahme einer Zuständigkeit des Verarbeitungsstaates könnte die Entscheidung schwieriger Vorfragen nötig machen, wenn die Daten in mehreren Ländern innerhalb des Konventionsgebietes einem Verarbeitungsvorgang unterzogen wurden.
- Werden beim Import Verknüpfungen mit originären Daten aus einem Konventionsstaat vollzogen, muss der Ursprungsstaat, aus dem Daten bezogen wurden, die Exporterlaubnis erteilen; würde die Kompetenz dem Importstaat belassen, könnte der Entscheid des Ursprungsstaates umgangen werden, indem beim Importland die Genehmigung für einen nachfolgenden Export eingeholt würde. Bei der Verknüpfung von Angaben aus mehreren Staaten muss ein aufgeteilter, sequentieller Import in die fraglichen Länder mit nachfolgendem genehmigten Export stattfinden.

Die mit diesem Lösungsmodell erreichte Verlagerung des Kollisionsproblemes auf die nationale Stufe bringt m.E. allen am grenzüberschreitenden Datenverkehr Beteiligten Vorteile:

- Den Konventionsstaaten erlaubt sie eine saubere Trennung des konventionsinternen und -externen Verkehrs mit einer klaren Zuständigkeitsregelung.
- Den datenverarbeitenden verantwortlichen Stellen bringt sie eine erleichterte Orientierbarkeit dank der Landesregisternummer; diese könnte ausserdem ev. über den Landescode auch für eine datensicherungsmässige Sperrung der Ausfuhr nicht originärer Daten eingesetzt werden.

- Dem Datensubjekt ermöglicht sie eine klare Vorstellung über die Vorschriften, die für den Export der ihn betreffenden Daten gelten: Der Betroffene wird regelmässig den Ursprungsort und das dort geltende Recht kennen, weil es meistens das Wohnsitzrecht ist. (Dabei kann allerdings nicht vermieden werden, dass auf Daten einer Person auch andere Rechte als die des Wohnsitzstaates anwendbar sein können, wenn sie ihren Ursprung im Ausland haben, z.B. im Zusammenhang mit Reisen: Kreditkarte, Hotelbuchungen, Flugreservierungen etc.).

D. Weitere Differenzierung der Drittstaaten

Das Prinzip der geschlossenen Konvention verunmöglicht grundsätzlich die Anwendbarkeit des Rechts eines Drittstaates, mag er auch ein noch so vollkommenes Datenschutzrecht haben, weil er nicht Mitglied der Konvention ist: Aus diesem Grunde scheint es mir wenig sinnvoll, die Drittstaaten für eine differenzierte Behandlung noch weiter in Staaten mit Datenschutzgesetzgebung und solche ohne datenschutzrechtliche Normen zu unterteilen. Durch die Zuweisung der Kompetenz zur Erteilung bzw. Verweigerung einer Export- oder Importgenehmigung an Drittstaaten, bleibt es dem Ursprungsstaat überlassen, in seinem nationalen Recht eine unterschiedliche Export- bzw. Importpraxis einzuführen.

§ 13 LOESUNGSVORSCHLÄGE FÜR DEN NATIONALEN BEREICH, INSBESONDERE
IM HINBLICK AUF EIN SCHWEIZERISCHES DATENSCHUTZRECHT

I. Vorbemerkung

1. In den vorangehenden Ausführungen sind an diversen Stellen Folgerungen gezogen worden, die zum Teil auf einer eingehenden Betrachtung verschiedener Aspekte beruhen und auch als Lösungsvorschläge konzipiert sind. Damit keine Redundanzen entstehen, wird auf die entsprechenden Stellen verwiesen, falls dort bereits eine ausführliche Darlegung und Begründung zu einem Lösungsvorschlag erfolgt ist. In diesem und dem folgenden Paragraphen sollen auch nicht nochmals alle Lösungspunkte aufgeführt werden; Zweck dieser abschliessenden Ausführungen ist es vielmehr, die wichtigsten Erkenntnisse zu einem abgerundeten Lösungsmodell zusammenzutragen.
2. Die Betrachtungen zur Regelung des grenzüberschreitenden Datenverkehrs haben gewisse Erkenntnisse über allgemeine Aspekte des Datenschutzes (z.B. Anwendungsbereich, Registrierung, etc.) gebracht. Diese Ausdehnung der Blickwinkel ist notwendig, weil das Konzept der Regelung des grenzüberschreitenden Datenverkehrs immer in Verbindung mit den allgemeinen Grundsätzen eines nationalen Datenschutzrechts gesehen werden muss. Die Wirksamkeit einer Regelung internationaler Verarbeitungsvorgänge bzw. der von einem Gesetz erreichte Schutzgrad von Personen bzw. deren Persönlichkeitsrechte nach erfolgtem Export von personenbezogener Information resultiert nicht allein aus den Bestimmungen zur Datenein- und -ausfuhr, sondern aus der Gesamtkonzeption eines nationalen Datenschutzrechtes. Aus diesem Grunde werden nicht nur die auf den grenzüberschreitenden Verkehr bezogenen Regeln behandelt, sondern auch jene allgemeinen Aspekte des Datenschutzes betrachtet, die de lege ferenda wünschbar erscheinen, um einen wirksamen Schutz auf nationaler und internationaler Ebene zu gewährleisten.

II. Grundsätzliche Ueberlegungen zu den allgemeinen Aspekten eines Datenschutzgesetzes

1. Ausgangspunkt^{1 2}

Leitgedanke bei der Ausgestaltung einer nationalen Regelung des grenzüberschreitenden Datenverkehrs sollte die Vorhersehbarkeit und Beurteilbarkeit der Rechtslage durch inländische und ausländische Stellen sein. Dies bedeutet gleichzeitig einen Grundsatzentscheid zugunsten des organisatorischen Lösungsmodells,³ welches nicht nur den Vorteil der erhöhten Rechtssicherheit in sich birgt, sondern gleichzeitig eine Angleichung an das deutsche und österreichische Gesetz bedeuten würde, womit eine einheitliche rechtliche Grundstruktur im deutschsprachigen Raum geschaffen würde, die allen am Informationsprozess aktiv oder passiv beteiligten Personen zugute käme.

Dabei ist Voraussetzung, dass der rechtlichen Ausgestaltung des grenzüberschreitenden Datenverkehrs die angemessene Bedeutung zugemessen und für den öffentlichen wie privaten Bereich eine klare Regelung getroffen wird, wobei den unterschiedlichen Wesensmerkmalen dieser beiden Sektoren entsprechende Beachtung zu schenken wäre.

2. Zielsetzung eines schweizerischen Datenschutzrechts⁴

Eine Datenschutzgesetzgebung soll nicht allein dem Schutz der Persönlichkeit vor Beeinträchtigungen durch die Verarbeitung personenbezogener Informationen dienen, sondern den Datensubjekten auch einen

1 Auf eine Aufzählung der Gründe für ein schweizerisches Datenschutzrecht kann verzichtet werden; sie sind in zahlreichen Publikationen ausführlich erörtert. Ausserdem unterstreichen die parlamentarische Initiative Gerwig vom 22.3.77 und die Vorarbeiten der Kommissionen Pedrazzini I und II, das das Ungenügen des geltenden Rechts durch eine Spezialgesetzgebung zum Datenschutz aufgehoben werden soll.

2 Ferner wird vorausgesetzt, dass ein nationaler Gesetzgeber, wie STADLER ausführlich erörtert (Online-adl. 11/77, S. 923), sich auch mit dem grenzüberschreitenden Datenverkehr auseinandersetzen muss, da dieser heute nicht mehr bloss Theorie, sondern Realität darstellt.

3 Vgl. vorne, S. 190.

Schutz ihres informationellen Selbstbestimmungsrechts⁵ garantieren. Nebst der Wahrung der Rechte der von der Datenverarbeitung betroffenen Subjekte gilt es, auch die Interessen und Rechte⁶ derjenigen natürlichen und juristischen Personen zu gewährleisten, die die Datenverarbeitung betreiben. Gegenüber den staatlichen Behörden wird ein Datenschutzgesetz nicht nur die Schranken der behördlicher Eingriffe in den Informationshaushalt festlegen. Es kann als Reflexwirkung auch dazu beitragen, dass den staatlichen Organen angemessene Informationen i.S. eines Informationsgleichgewichtes bereitgestellt und Lücken bei der Verwaltungskontrolle gefüllt werden.⁷ Die Ziel- funktion des Datenschutzes erschöpft sich somit nicht allein im Schutz der Persönlichkeit und der Grundrechte, sondern trägt durch Regelungen über den Bedarf und den Umgang mit Daten durch deren Erhebung, Verwendung und Weitergabe sowie mit den Anforderungen an

4 SCHWEIZER, Computer und Recht, S. 103.

5 Der Schutz der Privatsphäre bzw. der Schutz vor dem Eindringen in einen privaten persönlichen Bereich ist nur ein Aspekt der im Komplex "Persönlichkeitsrecht" zusammengefassten Ansprüche - ein mindestens ebenso wichtiger Aspekt ist die Garantie der individuellen Entfaltungsfreiheit (zur Konkretisierung vgl. EGGER, Art. 28 N 23, 26-46; GROSSEN, Einzelperson, S. 365; HINDERLING, S. 10ff.; HOTZ, S. 40f.; SCHUCAN, S. 13f.; ferner BGE 53 II 329, 79 IV 20; 84 II 277; 86 II 365; 88 II 174; 88 II 322). Diese individuelle Entfaltungsfreiheit ist zu verstehen als Meinungs- äusserungsfreiheit bzw. als Freiheit, über sich bestimmte, ge- wünschte Informationen verbreiten zu dürfen, d.h. die Möglich- keit zu haben, in der Aussenwelt bestimmte Abbildungen seiner selbst zu erzeugen und die Qualität der so erzeugten Abbilder in gewissen gesetzlichen Grenzen frei zu bestimmen (= informationel- les Selbstbestimmungsrecht), so dass der Einzelne die Möglich- keit hat, in der Umwelt je nach den Rollen, die er in verschie- denen sozialen Bereichen spielt, eine andere Facette seiner Per- sönlichkeit zu reflektieren. Dem Individuum muss mit dem informa- tionellen Selbstbestimmungsrecht die Möglichkeit gewährt werden, sich zu entfalten, zu entwickeln, d.h. sein Persönlichkeitsbild mit der Zeit zu ändern.

6 Meinungs- und Informationsfreiheit, Unternehmens- und Geschäfts- geheimnis, Handels- und Gewerbefreiheit, Persönlichkeitsrecht etc.

7 SCHWEIZER, a.a.O.

deren Richtigkeit, Vollständigkeit und Bindung an einen Kontext allgemein zu einer ordnungsgemässen, sorgfältigen Behandlung der geschützten Informationen bei.⁸

3. Anwendungsbereich i.w.S.⁹

A. Anwendungsbereich i.e.S.

Der Anwendungsbereich hat für den grenzüberschreitenden Datenverkehr insofern eine Bedeutung, als grundsätzlich in allen Bereichen des öffentlichen und privaten Sektors internationale Datenflüsse vorkommen können und demgemäss in beiden Sektoren ein unbestreitbares Schutzbedürfnis der Persönlichkeit zu registrieren ist.

Der private Bereich wird von den bestehenden Datenschutzgesetzen teils umfassend (d.h. mit Gültigkeit für alle im privaten Sektor die Verarbeitung personenbezogener Daten betreibenden Unternehmen oder Personen¹⁰), teils nur bereichsspezifisch (d.h. beschränkt auf einige Branchen privater Verarbeiter¹¹) geregelt. Aus diesen unterschiedlichen Regelungsformen der nationalen Gesetze entsteht hinsichtlich der internationalen Dimension leicht die Gefahr von Gesetzeslücken, die im transnationalen Verkehr für die verantwortliche Stelle und den Betroffenen nachteilige Folgen haben können. Es empfiehlt sich daher, einen umfassenden Schutz auf nationaler Ebene anzustreben und alle dem privaten Bereich angehörenden natürlichen oder juristischen Personen und Rechtsgebilde zu erfassen, die die personenbezogene Datenverarbeitung vollziehen (bzw. durch eine Verarbeitung in der Persönlichkeit betroffen werden können).

Im Hinblick auf ein schweizerisches Datenschutzgesetz steht dem Bund aufgrund von Art. 64 und Art. 32bis Abs.2 BV, sowie gemäss

8 MALLMANN, Zielfunktionen, S. 70ff.

9 Der Anwendungsbereich i.w.S. umfasst den Anwendungsbereich i.e.S., den Schutzbereich und den sachlichen Geltungsbereich des Gesetzes. In den nachfolgenden Ausführungen wird unter "Anwendungsbereich" immer die Bedeutung i.e.S. verstanden, d.h. der Anwendungsbereich eines Gesetzes auf den öffentlichen und/oder privaten Bereich.

10 Z.B. AU, BRD, F.

11 Z.B. DK, N, USA.

Art. 64bis, 34ter Abs.1, Art. 31quater und Art 34 Abs.2 BV die Befugnis zum Erlass von Datenschutzvorschriften für alle Bereiche des privaten Sektors zu,¹² so dass er sich im Interesse eines wirksamen Persönlichkeitsschutzes nicht auf eine bereichsspezifische Gesetzgebung im privaten Bereich beschränken sollte.

Im öffentlichen Bereich sind ebenfalls Lösungen verschiedenen Umfanges möglich. Die Ursache für Unterschiede im Anwendungsbereich liegt hier meist in der Struktur eines Landes, die in der grundrechtlichen Kompetenzverteilung zum Ausdruck kommt. So besitzt der Gesetzgeber zentralistisch organisierter Staaten die Befugnis zum Erlass von Vorschriften für alle Bereiche der öffentlichen Verwaltung, während für ein föderalistisch strukturiertes Land eine aufgeteilte Gesetzgebungskompetenz für die verschiedenen Gesetzgebungsstufen charakteristisch ist. Die Vor- und Nachteile dieser beiden Modelle im Kontext des Datenschutzrechts ist bereits an verschiedenen Stellen¹³ erläutert worden.

Das schweizerische Rechtssystem im öffentlichen Bereich ist durch das föderalistische Prinzip gekennzeichnet: Der Bundesgesetzgeber besitzt nur für den Bereich der Bundesverwaltung und die Rechtsträger öffentlicher Bundesaufgaben die Kompetenz zum Erlass von Datenschutzvorschriften; ferner ist er zur Schaffung von Normen aufgrund der speziellen Sachkompetenzen, der Organisationskompetenz (Art. 85 Ziff.1 BV) und den Kompetenzen gemäss Art. 103 und 106-114bis sowie nach Art. 117 BV ermächtigt.¹⁴ Dagegen ist eine verfassungsrechtliche Gesetzgebungskompetenz des Bundes im Bereich der kantonalen und kommunalen Organisationen und Verwaltungen nicht vorhanden, so dass die öffentlichrechtlichen Informations- und Organisationsregelungen auf kantonomer und kommunaler Stufe u.U. nicht im Einklang mit dem Bundesrecht vollzogen werden.

Hier stellt sich eine der grundlegendsten und delikatesten Fragen im Rahmen des schweizerischen Datenschutzrechts: Ist es ange-

12 SCHWEIZER, a.a.O., S. 107f.

13 Vgl. vorne, S. 133ff., 138ff., 158ff., und bes. 161ff.

14 Id., a.a.O., S. 108.

sichts der geographisch sehr beschränkten Ausdehnung der Schweiz und der kleinräumigen territorialen Struktur ihrer Gliedstaaten auch im speziellen Fall des Datenschutzes im öffentlichen Bereich angebracht, das föderalistische Prinzip zu verwirklichen oder wäre eine Ausnahmeregelung im Interesse des Persönlichkeitsschutzes geboten ?

Oesterreich hat zur Beantwortung dieser Frage eine gewisse Vorarbeit geleistet und dazu ein neues Modell der bundesstaatlichen Kompetenzverteilung geschaffen, indem es die Gesetzgebung für den Schutz der Privatsphäre ausschliesslich dem Bund übertrug.¹⁵ Leitgedanke war, dass einerseits für den Schutz der Privatsphäre ein einheitliches Schutzniveau in Bund, Ländern und Gemeinden sowie den Rechtsträgern und Selbstverwaltungskörper als notwendig erachtet wurde,¹⁶ und andererseits unterschiedliche Regelungen des Datenschutzes im öffentlichen Bereich wegen der geringen Grösse des österreichischen Staatsgebietes und der einzelnen Bundesländer unzweckmässig erschienen.¹⁷ Die Voraussetzungen und Ueberlegungen, die zu dieser Neuverteilung der Kompetenz geführt haben, treffen auch für die schweizerischen Verhältnisse zu:

- Die gegenüber Oesterreich geographisch noch kleinräumiger strukturierte, föderalistische Landschaft würde den von der Datenverarbeitung im öffentlichen Bereich betroffenen Bürger durch unterschiedliche Schutzvorschriften¹⁸ (auf Gemeinde-, Kantons- und Bundesebene) stark belasten.
- Die Gefahr der Rechtszersplitterung ist gross, wenn nicht durch interkantonale Vereinbarungen (Konkordate) oder durch Einigung auf Mustervorschriften eine minimale Rechtsvereinheitlichung herbeigeführt wird.
- Eine Vereinheitlichung¹⁹ des Datenschutzrechts im öffentlichen

15 Vgl. vorne, S. 158ff. und dort genannte Quellen.

16 STADLER, Verwaltungspraxis, S. 12.

17 REISINGER, DS+DS 2/79, S. 120.

18 LDSG von Rheinland-Pfalz und Hessen schützen z.B. auch juristische Personen, BDSG und andere LDSG nicht; vgl. ferner 2. Tätigkeitsbericht d.B.f.D., Nr. 4.4: Abweichendes Landesrecht, S. 67ff.

19 Ebenso PODLECH, S. 4f.

Bereich ist m.E. nicht nur aus den obgenannten Gründen, sondern auch zur Sicherstellung eines wirksamen Datenschutzes gegenüber der öffentlichen Verwaltung angebracht. Für den innerschweizerischen Datenfluss zwischen Bundes-, Kantons- und Gemeindebehörden könnte die Rechtsvielfalt und die Bindung an das Legalitätsprinzip zu Inkompatibilitäten führen, aber auch im Verkehr zwischen privaten und öffentlichen Stellen sind Probleme vorstellbar.

- Nachdem diese Probleme schon auf nationaler Ebene den Datenfluss und die Wirksamkeit der Datenschutznormen bedrohen, könnten sie sich im internationalen Rahmen weit mehr als Belastung für das schutzberechtigte Datensubjekt und die am DV-Prozess beteiligten Personen auswirken. Hier wird nicht nur die durch die Rechtszersplitterung verursachte Rechtsunsicherheit zum Hindernis, sondern auch die kantonale und kommunale Organisationsautonomie und die dadurch bewirkte Vielfalt von Aufsichtsbehörden.²⁰ Dabei würde nicht allein der im öffentlichen Sektor stattfindende grenzüberschreitende Datenverkehr betroffen, sondern auch denjenigen, welchen verantwortliche Stellen aus beiden Bereichen austauschen.
- Schliesslich spricht m.E. auch eine grundsätzliche Betrachtung für eine einheitliche Regelung des Datenschutzes im Bundesstaat: Der Föderalismus sollte dazu dienen, regionale Unterschiede zu berücksichtigen, die bei der behördlichen Organisation und Kompetenzaufteilung vorhanden sein können, ihren Niederschlag aber nicht in der Materie des Datenschutz haben. Das staatsrechtliche Prinzip des Föderalismus sollte nicht dazu dienen, eine Begrenzung oder unterschiedliche Ausgestaltung des Schutzes der Persönlichkeit und der Grundrechte des Einzelnen gegenüber den verschiedenen Verwaltungskörpern zu rechtfertigen.

Bei den noch anstehenden gesetzgebungstechnischen und gesetzgebungs politischen Ueberlegungen sollte letztlich allein das Schutzbedürfnis der einzelnen Person gegenüber der Verwaltung und das Interesse an einer wirksamen Verbesserung des Datenschutzes ausschlaggebend sein.

²⁰ Z.B. im Hinblick auf die Deklaration und Bezeichnung dieser Stellen in einer internationalen Konvention, wie es in Art. 13 KE vorgesehen ist.

B. Bereich der geschützten Subjekte (Schutzbereich)

Das hier anstehende Problem der Konzeption des Datenschutzes betrifft das Schutzobjekt, d.h. die Entscheidung über die Verwirklichung des Individualdatenschutzes oder eines Kollektivdatenschutzes. Die datenschutzrechtliche Relevanz personenbezogener Angaben über natürliche Personen ist Ausgangspunkt des Datenschutzes und allgemein anerkannt, hingegen ist der Schutz personenbezogener Daten über juristische Personen in den existierenden Datenschutzgesetzen und -entwürfen unterschiedlich verwirklicht.²¹ Dementsprechend bestehen die wohl erheblichsten Meinungsunterschiede und datenschutzrechtlichen Auswirkungen in der Beantwortung der Frage, ob die nationale Gesetzgebung bzw. eine internationale Konvention ebenfalls auf Daten von juristischen Personen oder Personengruppen ohne Rechtspersönlichkeit Anwendung finden soll. Es gibt eine Vielzahl von Gründen, die pro und contra eine Ausdehnung des Schutzes auf die Daten von juristischen Personen und Personengruppen sprechen.²²

a) Schutz von Daten juristischer Personen

aa) Argumente für eine Ausdehnung des Schutzes²³

- Der fehlende Schutz kann den Unternehmer, der für seine Geschäftstätigkeit eine entsprechende Gesellschaftsform²⁴ gewählt hat, benachteiligen:
 - Seine Konkurrenten, die als natürliche Personen, (z.B. als Einzelkaufmann) ihre Geschäftsziele verfolgen, profitieren vom Schutz der auf sie - sowohl als Geschäftsperson wie als Privatperson - bezogenen Daten, die er als Unternehmer, der

21 Schutz nur natürlicher Personen in: Europarat-Resolutionen (73) 22 und (74) 29, BDSG in BRD, Frankreich, Privacy Act in USA. Schutz natürlicher und juristischer Personen in: Oesterreich, Dänemark, Länder-Datenschutzgesetze in Rheinlandpfalz und Hessen (in Abweichung vom BDSG).

22 Vgl. vorne, S. 136, 140f. und 163f.

23 Vgl. auch Argumente bei Konvention des Europarates, vorne, S. 244.

24 Z.B. Einmann AG oder personalistisch konzipierte Gesellschaftsform.

Rechtspersönlichkeit seiner Gesellschaftsform wegen, nicht genießen kann.

- Grosse multinationale Gesellschaften haben bei einem fehlenden Schutz der auf sie bezogenen Daten, aufgrund ihrer wirtschaftlichen Macht und der Möglichkeit internationaler Verknüpfungen, gewisse Selbstschutzmöglichkeiten, während das eindimensional strukturierte, auf den nationalen Bereich beschränkte Unternehmen solcher Mittel und Möglichkeiten entbehrt.
- Aus Daten, die eine kleinere Gesellschaft betreffen, können oft Rückschlüsse auf ihren Besitzer gezogen werden, weil sie von der Person des Inhabers praktisch nicht trennbar sind; solche Informationen enthalten demzufolge oft auch Angaben mehr oder weniger sensibler Natur über natürliche Personen. Es ist sogar eine Speicherung von personenbezogenen Informationen über den Alleinaktionär oder eine kleine Zahl von Eigentümern unter dem Namen der juristischen Person möglich, so dass diese unter dem Mantel der juristischen Person über deren Führungsorgane gespeicherten Angaben wegen des fehlenden Schutzes von juristischen Personen ungeschützt bleiben müssten. Auch die Individualkontrolle ginge verloren, wenn die juristischen Personen dem Schutzbereich nicht unterstehen und deshalb keine Individualrechte zu ausüben können. Personenbezogene Daten könnten somit leicht unter einer Tarnung als Firmendaten gespeichert werden, weil Firma und Besitzer identisch sind.²⁵ Dadurch könnte eine Grauzone und ein Rechtsvakuum für diese Art von Rechtssubjekten entstehen.

Aus dieser Darstellung wird ersichtlich, dass gerade von den Personenverbindungen mit Rechtspersönlichkeit, d.h. den Gesellschaftsformen mit personalistischem Element ein starkes Schutzbedürfnis der auf juristische Personen bezogenen Daten ausgeht. Obwohl bei den kapitalbezogenen Gesellschaften die Individualität mehr oder weniger bedeutungslos ist,²⁶ hat auch hier der Schutz der Daten seine Berechtigung, wenn man bedenkt, welche wirtschaftlichen und rechtlichen Auswirkungen ein Missbrauch auf andere juristische und natürliche Personen haben kann.

- Sowohl bei den personalistisch konzipierten als auch bei den kapitalbezogenen Gesellschaftsformen ergibt sich, dass Dateien, die grundsätzlich juristische Personen betreffen, nicht ausschliesslich Informationen über die Gesellschaft, sondern auch Angaben über natürliche Personen enthalten können, die in einer bestimmten Beziehung zur Gesellschaft stehen.^{27 28} Wenn solche Daten ausserhalb des Geltungsbereiches der Datenschutzgesetzgebung verbleiben, wird es nie eine effektive Kontrolle über das Ausmass der Gefährdung der individuellen Privatsphäre geben. Die ohnehin schwer zu ziehende Trennung zwischen personen- und sachbezogenen Daten wird durch die zusätzliche Differenzierung zwischen juristischen und natürlichen Personen noch komplizierter und undurchschaubarer, so dass trotz rechtlichen Schutzes der natürlichen Personen ein Vakuum im Ueberschneidungsbereich mit den juristischen Personen entstehen kann.
- Aufgrund der wechselseitigen wirtschaftlichen, politischen und sozialen Abhängigkeiten und Verflechtungen von Wirtschaft, Industrie, Staat und Individuen, ist auch ein Schutz der personenbezogenen Daten juristischer Personen zu befürworten. Innerhalb dieser Interdependenzen besteht ein natürliches Schutzbedürfnis der Gesellschaften, primär gegenüber staatlichen Eingriffen, andererseits aber auch gegenüber Vertragspartnern und Mitbewerbern; ein entsprechendes Bedürfnis existiert bei staatlichen Institutionen vor Verletzungen durch private Gesellschaften und Interessengruppen. So sind Kontrollrechte wie z.B. das Einsichts- bzw. Auskunftsrecht für juristische Personen ebenso bedeutsam, wie für eine natürliche Person, wenn es darum geht, die Richtigkeit der sie betreffenden Angaben zu überprüfen, diese Daten zu korrigieren und deren Verwendung

25 Vgl. TDR, Vol. 1, No. 1, S. 4.

26 MEIER-HAYOZ/FORSTMOSER, S. 83 N 8.

27 Z.B. als Organe einer juristischen Person.

28 DUSCHANEK führt ganz allgemein zur Begründung auf, dass die Mehrheit der Informationen über eine juristische Person sich auf Informationen über eine natürliche Person zurückführen lässt (§ 3 DSG, S. 19).

auf Missbräuche hin zu prüfen. Die Individualrechte anderer (natürlicher oder juristischer) Personen dürfen aber nicht soweit gehen, dass bei deren Ausübung die Persönlichkeitsrechte der bearbeitenden Stelle verletzt werden, wie z.B. das Geschäftsgeheimnis: Dies bedeutet eine Beschränkung des Einsichtsrechts oder des Auskunftsrechts gegenüber Daten, die dem persönlichen oder geschäftlichen Geheimbereich der verarbeitenden natürlichen oder juristischen Person angehören.²⁹

Schutzlosigkeit der auf juristische Personen bezogenen Informationen kann bei Missbräuchen infolge der internationalen Interdependenz erhebliche Auswirkungen auf die einzelnen Staaten in wirtschafts- und sozialpolitischer Beziehung haben und die persönlichen Rechte der Individuen gefährden.

- Innerhalb des grenzüberschreitenden Datenverkehrs ist ein grosser Teil der Daten auf Individuen bezogen, wie z.B. im Banken- und Versicherungswesen, Kredit- und Reisegeschäft usw.; noch grösser ist aber der Umfang an sensibler geschäftlicher Information innerhalb des Bereiches des internationalen Handels. Dieses grosse Volumen an Geschäftsdaten, welche detaillierte Kunden- und Klientendaten oder vertrauliche Geschäftsinformationen enthalten können, erfordert einen Schutz auf nationaler wie internationaler Ebene, da bei einer unterschiedlichen Grenzziehung zwischen Geschäfts- und Individualdaten die letzteren allzu leicht, als "Geschäftsdaten" deklariert und damit der Schutzlosigkeit preisgegeben werden könnten. Im internationalen wie nationalen Bereich dürfen keine Auslegungsunterschiede unter dem Deckmantel der Geschäftsinformation juristischer Personen zur "legitimen Schutzlosigkeit" von Individualdaten und damit zu neuen Datenhindernissen infolge nationaler Abwehrmassnahmen führen.

29 Vgl. hinten, S. 343.

bb) Argumente gegen eine Ausdehnung des Schutzes³⁰

- Am häufigsten wird das Argument vorgebracht, juristische Personen seien unter verschiedenen anderen Aspekten der nationalen Rechtsordnung geschützt.³¹ Diese Argumentation mag innerhalb des nationalen Bereiches berechtigt sein, hilft aber im Rahmen des grenzüberschreitenden Datenverkehrs nichts, denn diese Schutzaspekte variieren von Land zu Land und vermögen im internationalen Bereich keinen einheitlichen Damm gegen die Gefahr eines Missbrauches von personenbezogenen Daten über juristische Personen aufzurichten. Dabei ist m.E. sehr fraglich, ob die bestehende Gesetzgebung überhaupt zum Schutz von Daten juristischer Personen ausreicht, wenn von der schweizerischen Gesetzgebung³² gesagt werden kann, dass die geltenden Bestimmungen zum Schutz der Persönlichkeit³³ "gegenüber dem Schädigungspotential moderner ADV praktisch wirkungslos" sind.³⁴ Wirkungslos, weil sowohl die öffentlichrechtliche als auch die in der generalklauselartigen Form des Art. 28 ZGB gestaltete zivilrechtliche Grundlage aus einer Zeit vor der Entwicklung der automatischen Datenverarbeitung und der damit verwandten Technologien stammt. Ausserdem sind angesichts der Zielfunktion des Datenschutzes zahlreiche Lücken und Mängel in der bestehenden

30 Vgl. EUROPEAN PARLIAMENT, in: TDR, Vol. 2, No. 2, S.17f.

31 Z.B. Schutz des Geschäftsgeheimnisses (StGB 162).

32 Die schweizerische Rechtsordnung schützt gemäss Lehre und Rechtsprechung auch die Persönlichkeit juristischer Personen.

33 Art. 27, 28 i.V. Art. 53 ZGB

34 SCHUCAN, S. 111; FORSTMOSER, Grundfragen und Lösungsmöglichkeiten, S. 36: "...das geltende Recht vermag nicht zu genügen..."; HAUSHEER schreibt allgemein: "... sei ausdrücklich festgehalten, dass die Notwendigkeit der Verstärkung des Schutzes der Persönlichkeit mit den Mitteln des Zivilrechts im Lichte der heutigen gesellschaftlichen und sozialen, technischen und wirtschaftlichen Verhältnisse ganz überwiegend anerkannt wird" (S. 82), ferner "übereinstimmend wird auch anerkannt, dass die Generalklausel von Art. 28 ZGB den besonderen technischen Gegebenheiten gewisser Datensammlungen allein nicht mehr zu genügen vermag..." (ebenda, S. 94).

Rechtsordnung erkennbar:

- Es fehlen einfache allgemeine Normen, die die Individualkontrolle garantieren und dabei insbesondere den Umfang eines Einsichts- und Auskunftsrechts für das Datensubjekt festlegen.
- "Materielle Grundsätze für die Informationsbeschaffung, -verarbeitung und -verbreitung sind bisher nur ungenügend entwickelt oder zur Geltung gebracht worden."³⁵
- Es existieren keine präventiven und repressiven Massnahmen zur Fremdkontrolle der DV, noch gibt es Vorschriften über die Selbstkontrolle durch die für die Datenverarbeitung verantwortliche Stelle, damit ein wirksamer Datenschutz entstehen kann.

Neben Lücken und Mängeln gibt es im bestehenden Recht auch Vorschriften, die mit einem wirksamen Datenschutz inkompatibel sind oder ihm entgegenstehen, wie z.B. bundesrechtliche Erlasse über Statistiken oder internationale Vereinbarungen mit umfassenden Datenerhebungs Kompetenzen und Auskunftspflichten.

- Zur Unterstützung unternehmerischer Entscheidungen werden innerhalb einer Gesellschaft die verschiedensten Erhebungen und Auswertungen vorgenommen. In einem Fertigungsbetrieb z.B. können statistische Angaben über die Produktion einzelner Bestandteile von Zulieferfirmen geführt werden, auf denen auch Einschätzungen über die mögliche Leistung und die Leistungsfähigkeit des Lieferanten basieren, die für eine Steigerung der Produktion, für eine Beurteilung der Rentabilität und Kostenrechnung, für den Entscheid über die Wahl neuer Lieferanten oder zugunsten einer Selbstproduktion solcher Bestandteile entscheidend sein können. Wenn aber statistische Angaben und Dateien dieser Art den betreffenden Lieferanten zur Einsicht offenstehen müssen und ihnen der Verarbeitungszweck bekanntzugeben wäre, könnten geschäftliche Verbindungen und Beziehungen gestört oder sogar geschädigt werden.

35 SCHWEIZER, Computer und Recht, S. 104.

- Ebenso nachteilig kann die Transparenzpflicht sich gegenüber betroffenen juristischen Personen auswirken, wenn in einem Unternehmen Informationen über die Aktivitäten und Verkaufserfolge von Konkurrenzfirmen gesammelt werden, die als Entscheidungsgrundlage für bestimmte Verkaufs- und Marketingstrategien dienen. Eine ähnliche Gefährdung der Wettbewerbsfähigkeit einzelner Unternehmen könnte durch ein Einsichtsrecht der Konkurrenz in geschäftsintern erarbeitete Marktforschungsdaten ³⁶ und -dateien mit auf juristische und natürliche Personen bezogenen Angaben bewirkt werden.

Diese letzten beiden Argumente wiegen schwer gegen eine Verwirklichung des Schutzes von Daten juristischer Personen, wenn die individuellen Kontrollrechte der juristischen Person gleich ausgestaltet werden wie die Ansprüche der natürlichen Person.

Hier wird der Konflikt zweier Ausschlussrechte sichtbar, was eine Wertabwägung erheischt: Auch juristische Personen verfügen über

36 In diesem Zusammenhang ist das Referat von Robert Schweizer über BDSG und Länderdatenschutzgesetze und deren Folgen für Markt- und Sozialforschungsinstitute vor dem Verband schweizerischer Marktforscher (VSMF) [am 21.11.1979 in Zürich] erwähnenswert: Das Hauptprinzip des deutschen Datenschutzes besteht im grundsätzlichen Verbot der Verarbeitung personenbezogener Daten, das für eine Erhebung einen Rechtfertigungsgrund erfordert, der im einzelnen Datenschutzgesetz selbst, einem andern Gesetz oder in der Zustimmung des betroffenen Subjektes liegen kann. "Inwieweit diese Regelung die Marktforschung behindern kann, illustriert der Referent an einem fiktiven Beispiel: Eine Markterhebung für die CSU würde durchgeführt mit dem Ziel, festzustellen, wie sich die Popularität von Franz Josef Strauss erhöhen liesse. Jedem Befragten müssten zuerst die Ziele der Erhebung klargelegt werden, um darauf dessen schriftliche Zustimmung für die Weiterverarbeitung der Daten zu erhalten. Als Folge wäre eine derartige Untersuchung wertlos. Für die Marktforscher sei nicht die Person relevant, sondern deren Meinung. Um der Zuverlässigkeit der Interviews willen seien Stichproben unerlässlich. Um Stichproben durchführen zu können, seien die Marktforscher auf Personaldaten angewiesen. Eine vollständige Anonymisierung der Daten sei somit nicht möglich." (NZZ Nr. 272/1979, S. 22).

eine geschäftliche³⁷ Privatsphäre, die sich aus dem von Dok-
trin³⁸ und Praxis³⁹ anerkannten allgemeinen Persönlichkeits-
recht ergibt, wobei der Persönlichkeitsbereich naturgemäss weniger
ausgedehnt ist, als der einer natürlichen Person.⁴⁰ Die geschäft-
liche Privatsphäre sollte Raum für unternehmerische Entscheidungsfindung,
und die Verarbeitung der dazu erforderlichen Wirtschaftsinformationen
und -analysen gewähren und muss von einer Offenlegungspflicht gegen-
über Dritten und vom Einsichtsrecht des Datensubjektes ausgenommen
werden. Dieser Freiraum wird durch die Konkretisierung der persön-
lichen Verhältnisse des allgemeinen Persönlichkeitsrechts unter-
mauert, indem den juristischen Personen eine ihrem Gesellschaftszweck
entsprechende Entfaltungsmöglichkeit zugesprochen wird.⁴¹ Da Daten-
schutz als "Schutz der Privatsphäre gegen Missbrauch von Daten über
Personen" definiert ist,⁴² bezweckt er den Schutz des Menschen und
seiner Privatsphäre, wie auch des Geheimbereichs juristischer Perso-
nen und Organisationen. Im Konfliktfall muss daher der Schutz der
Daten, die im Rahmen des Gesellschaftszweckes verarbeitet werden und
personenbezogene Informationen über die anfragende Person enthalten,
für die verarbeitende juristische Person aber ein wirtschaftlich ge-
heimzuhaltendes Faktum darstellen, den individuellen Rechten des

37 Auch nichtgeschäftliche Privatsphäre, entsprechend idealem oder wirtschaftlichem Zweck.

38 BAER, S. 100ff.; GROSSEN, Einzelperson, S. 289; HINDERLING, S. 28ff.; JAEGGI, S. 168a, 217a; TUOR/SCHNYDER, S. 77f.

39 BGE 95 II 488 E. 4; 97 II 99 E. 2.

40 Art. 53 ZGB.

41 HINDERLING, S. 10f.; vgl. auch WESTIN, Der Mensch und seine Privatsphäre, S. 289 mit anderer Argumentation, aber gleichgerichteter Folgerung bezüglich des Freiraums einer juristischen Person: "So wie der einzelne darauf angewiesen ist, sich in seine Privatsphäre zurückziehen zu können, um nicht unentwegt 'soziale Rollen' verkörpern zu müssen oder um gelegentlich einmal - in zulässigen Grenzen - von der gesellschaftlichen Norm abzuweichen, so braucht auch eine Organisation das Mass an interner Handlungsfreiheit, um einmal das üblicherweise für die Öffentlichkeit zur Schau getragene 'offizielle Gesicht' entspannen zu können."

42 NAGEL, S. 10.

Datensubjektes vorgezogen werden. Die Ausübung der Individualrechte durch Datensubjekte, die u.U. zugleich wirtschaftliche Konkurrenten darstellen, darf nicht zu einer Gefährdung der unternehmerischen Geheimsphäre und einer Beeinträchtigung des Wettbewerbs führen. Hier ist m.E. eine spezielle Vorschrift hinsichtlich der Geltendmachung von Individualrechten gegenüber den juristischen Personen angebracht, die der juristischen Person ein Verweigerungsrecht für diejenigen Datensätze einräumt, die dem geschäftlichen Geheimbereich angehören und deren Preisgabe eine Persönlichkeitsverletzung der juristischen Person selbst bedeuten würde. Das Unternehmen, welches von diesem Verweigerungsrecht Gebrauch macht, könnte z.B. verpflichtet werden, allgemeine Angaben über die zum geschäftlichen Geheimbereich gehörenden Daten zu machen, sofern dies mit dem Geschäftsgeheimnis zu vereinbaren ist. U.U. müsste einer unabhängigen Schiedsbehörde (Datenschutzbehörde) das Entscheidungsrecht zugestanden werden, damit bei Grenzfällen eine neutrale Interessenabwägung erfolgen kann.

b) Schutz von Daten, die Personengruppen und Rechtsgemeinschaften ohne Rechtspersönlichkeit betreffen

Der Gruppendatenschutz ist umstritten;⁴³ m.E. benötigen Personengruppen und Rechtsgemeinschaften ebenfalls einen Schutz der sie betreffenden Daten, auch wenn sie keine Rechtspersönlichkeit haben. Rechtsgemeinschaften bei denen das körperschaftliche Element der Mitgliedergesamtheit stark betont wird, rücken in die Nähe der juristischen Person, sind aber nicht rechtsfähige, juristische Personen, "sie werden nur in gewissen Bereichen so behandelt, wie wenn sie es

43 Ablehnend: SEIDEL, S. 71.

Befürwortend: EUROPEAN PARLIAMENT, TDR, Vol. 2, No. 2, S. 18; DUSCHANEK, § 3 DSG, S. 19; SCHUCAN, S. 26ff.; STEINMUELLER hielt in seinem Vortrag (zum Thema Datenschutz, gehalten an der Universität Zürich am 30.5.1975) den Schutz von Personengruppen für wichtiger als den Individualdatenschutz (zit. SCHUCAN, a.a.o.).

wären".⁴⁴ Aus dem fließenden Übergang von juristischen Personen zu "relativ juristischen Personen"⁴⁵ i.S. von Rechtsgemeinschaften ohne Rechtspersönlichkeit und weiter zu Personengruppen ohne jede rechtliche Grundlage, wird die Schwierigkeit der Grenzziehung deutlich. Personengruppen sind durch die Tatsache charakterisiert, dass sie sich entweder als Rechtsgemeinschaft mit vertraglicher Grundlage, (z.B. als Familie, Konsortium) oder als Gruppe mit gemeinschaftlichen Interessen oder Merkmalen (z.B. als geschiedene Frauen, Schulkinder, Parlamentarier etc.) gegenüber der Umwelt abheben. Wenn ungenaue oder falsche Angaben, die eine bestimmte Gruppe oder eine Rechtsgemeinschaft betreffen, publiziert werden, kann ein Individuum, das als zur Gruppe gehörig klassifiziert wird, u.U. erhebliche Nachteile erleiden und in seiner Persönlichkeit verletzt werden. Gemeinschaften, deren Mitglieder sich zur Verfolgung eines gemeinsamen Zweckes mit vereinten Mitteln und Kräften entschlossen haben, müssen in ihrer Eigenschaft als Personengesamtheit geschützt werden, auch wenn jeder einzelne Angehörige der Gruppe oder der Rechtsgemeinschaft in seiner Individualität und seinem Recht auf Entfaltung seiner wirtschaftlichen Persönlichkeit geschützt ist.⁴⁶ Wenn auch diese Personenzusammenschlüsse jeder Rechtspersönlichkeit entbehren, so besteht bei diesen Gebilden trotzdem ein klares Bedürfnis nach Berücksichtigung durch den Datenschutz sowohl in einer künftigen nationalen Gesetzgebung wie in einem internationalen Abkommen.

c) Folgerung

In der Erkenntnis, dass die Menschen gerade in der Gruppe ihre wertvollsten Ziele verwirklichen⁴⁷ - irrelevant ob mit oder ohne Rechtspersönlichkeit - und die Datenverarbeitung auch eine Bedrohung von Kollektivinteressen darstellen kann,⁴⁸ werden die bei Personen-

44 Vgl. MEIER-HAYOZ/FORSTMOSER, S. 60f.

45 Id., a.a.O.

46 Vgl. BGE 86 II 365; GROSSEN, Einzelperson, S. 375.

47 JAEGGI, S. 217a; SCHUCAN, S. 27.

48 DUSCHANEK, § 3 DSG, S. 19.

gruppen (v.a. juristischen Personen) anders gelagerten Schutzbedürfnisse evident. Die bei der juristischen Person unterschiedlich ausgelegte Privatsphäre verdeutlicht ferner, dass nicht die gleichen Massstäbe und Begriffe wie bei Individuen angelegt werden können. Eine Ausdehnung der Individualrechte aus dem Datenschutz auf Personen- und juristische Personen ergibt Inkompatibilitäten und Interessenkollisionen, die als berechtigte Argumente gegen eine Ausdehnung des Schutzes vorgebracht werden können.⁴⁹ Der Gruppendatenschutz bedarf einer speziellen, auf die Bedürfnisse dieser Gebilde zugeschnittenen Regelung. Die Verwirklichung eines umfassenden Schutzes der Persönlichkeit und die komplexen Wechselwirkungen zwischen der internationalen Wirtschaft, dem Staat und den Individuen rechtfertigen die Schaffung von speziellen Bestimmungen und Rechten auf nationaler wie internationaler Ebene, die der allgemeinen Zweckbestimmung und Interessenkonstellation solcher Gruppen- und Rechtsgebilde Rechnung trägt.

Die von multinationalen Gesellschaften vorgebrachten Bedenken, dass mit einer Erweiterung des Begriffes der personenbezogenen Daten auf juristische Personen den Behörden im Zusammenhang mit den Bestimmungen zum grenzüberschreitenden Datenverkehr die Möglichkeit gegeben werden könnte, den Fluss wirtschaftlicher Informationen zu überwachen, auch wenn keine Gefährdung von individuellen Persönlichkeitsrechten mit diesen Daten verbunden wäre,⁵⁰ ist durchaus berechtigt. Diese Befürchtungen sprechen einerseits wiederum für eine spezielle Regelung des Schutzes von Daten juristischer Personen, die solche Interventionen ausschliessen sollte, andererseits veranschaulicht sie die Bedeutung eines internationalen Rechtsregimes, innerhalb dessen Geltungsbereich ein freier Informationsfluss existieren sollte und

49 Einige Datenschutzgesetze schützen die Daten, die sich auf juristische Personen beziehen auf gleiche Weise und mit den gleichen Mitteln wie Daten, die natürliche Personen betreffen.

50 CARMODY, Information Privacy, Vol. 1, No. 1, S. 27, ferner Anm. 28/29, S. 29.

eine spezielle Genehmigungspflicht nur beim Verlassen des internationalen Schutzbereiches notwendig wäre. Unter diesen Voraussetzungen hätte m.E. eine Ausdehnung des Schutzes auf Daten über juristische Personen weder negative Auswirkungen auf Industrie und Handel, noch auf die betreffenden juristischen Personen bzw. Personengruppen.

Für ein schweizerisches Datenschutzrecht ist der Schutz von Daten, die juristische Personen betreffen, nicht allein aus den vorgenannten Gründen ⁵¹ zu befürworten, sondern aus der Ueberlegung, dass der Datenschutz am geltenden Recht anknüpfen und dessen Grundkonzeption des Persönlichkeitsschutzes weiterführen sollte. In der schweizerischen Rechtsordnung ist das allgemeine Persönlichkeitsrecht juristischer Personen (mit idealem oder wirtschaftlichem) Zweck von Doktrin ⁵² und Praxis ⁵³ anerkannt; es würde eine Zäsur entstehen und zu Unvereinbarkeiten im schweizerischen Persönlichkeitsrecht führen, wenn den juristischen Personen hinsichtlich der Datenverarbeitung die Persönlichkeitssphäre und deren Schutz abgesprochen würde.

Der Kollektivdatenschutz betrifft hingegen nicht nur die juristischen Personen, sondern auch Personenzusammenschlüsse und Vereinigungen ohne eigene Rechtsfähigkeit. Unter der geltenden Rechtsordnung sind sie aber nicht Träger des Persönlichkeitsrechts und können daher nicht in ihrer Persönlichkeit verletzt werden. ⁵⁴ De lege ferenda sollte aber auch der Schutz solcher Kollektive in das Datenschutzrecht einbezogen werden und diese Personengesamtheiten im Interesse der einzelnen Individuen schützen.

C. Sachlicher Geltungsbereich ⁵⁵

Für den Schutz der Daten wird in manchen Gesetzen ⁵⁶ unterschieden, ob sie mit automatisierten oder herkömmlichen, d.h. manuellen Verfahren bearbeitet werden. Für einen umfassenden Schutz der

⁵¹ Vgl. vorne, S. 337ff. und 262ff.

⁵² BAER, S. 100ff.; GROSSEN, Einzelperson, S. 289; HINDERLING, S. 28ff.; JAEGGI, S. 168a, 217a; TUOR/SCHNYDER, S. 77/78.

⁵³ BGE 95 II 488 Erw. 4, 97 II 99 Erw. 2.

⁵⁴ Gutachten des Max-Planck-Instituts, S. 329.

⁵⁵ Vgl. auch Ausführungen vorne, S. 136, 141ff., 164ff., 246ff. und 273.

Daten ist m.E. der Geltungsbereich eines Gesetzes auf beide Verfahrensarten auszudehnen. Unter den automatisierten Verfahren ist die elektronische Datenverarbeitung, ebenso wie die Bearbeitung mit automatischen und technischen Hilfsmitteln, mit Geräten der mittleren Datentechnik und mechanisierten Anlagen zu verstehen. Dabei muss Raum für heute noch nicht abzusehende technische Entwicklungen der Zukunft offen bleiben, damit neue Techniken und Verfahren ebenfalls unter dem sachlichen Geltungsbereich eines Gesetzes unterstellt werden können.

M.E. sind die manuellen Verfahren ebenfalls in den Anwendungsbereich (i.w.S.) des Gesetzes einzubeziehen, damit für den Umgang mit personenbezogenen Daten alle schutzrelevanten Phasen abgedeckt werden können und bei einer Beschränkung auf automatische Verfahrensarten kein Ausweichen auf manuelle Techniken zwecks Umgehung der Vorschriften möglich ist.

Bezüglich der manuellen Verfahren muss nun unterschieden werden zwischen manuellen Handlungen, die eine Ueberführung der Daten in die automatische Verarbeitung bezwecken und manuell bearbeiteten Datensammlungen, die in keiner Phase der Verarbeitung von automatischen Hilfsmitteln unterstützt werden. Die letztere Gruppe umfasst einen grossen Teil der heute existierenden Dateien mit personenbezogenen Daten und wird auch in Zukunft mit manuellen Verfahren unterhalten, so dass nicht einzusehen ist, weshalb diese nicht unbeträchtliche Zahl von gespeicherten Daten vom Schutzbereich ausgenommen werden soll. M.E. kann aber für solche Datensammlungen, bei welchen alle Verarbeitungsphasen ausschliesslich manuell erfolgen, eine besondere, mildere Regelung erlassen werden,⁵⁷ und zwar hinsichtlich des

-
- 56 Schutz manuell und automatisiert verarbeiteter Daten: BRD, N, AU (Verfassungsartikel), DK (priv. Bereich), RL.
Schutz nur automatisiert verarbeiteter Daten: F, LUX, AU, S, KE, DK (öffentlicher Bereich, aber mit Ausdehnungsmöglichkeit).
- 57 Datenschutzregeln sind angebracht, weil auch von Datensammlungen, die mit manuellen Verfahren erstellt werden, Persönlichkeitsverletzungen ausgehen können (vgl. Fall CINCERA); hingegen lässt sich für solche Dateien eine gesonderte Behandlung vertreten, weil die automatisierten Verarbeitungsphasen eine auf die

Datenschutzes, vor allem aber bezüglich der erforderlichen Datensicherungsmassnahmen. Allerdings muss im Interesse der Praktikabilität eines Gesetzes eine klare Grenzziehung zu den für den persönlichen Gebrauch bestimmten Verzeichnissen, Registern, Karteien und Notizbüchern vorgenommen werden.

Umgekehrt ist die andere Gruppe der manuellen Verfahren, die als manuell durchzuführende Vor-, Zwischen- oder Schlussphase in Verbindung mit irgendeinem automatischen Datenverarbeitungsvorgang stehen, als qualifizierte Datenverarbeitungshandlung dem Schutz des Gesetzes zu unterstellen. Dies bedeutet, anders ausgedrückt, dass in den sachlichen Geltungsbereich zu den verschiedenen Phasen der automatischen Verarbeitung (Erfassung, Speicherung, Verarbeitung, Uebermittlung, Löschung etc.) auch bestimmte Vorgänge der manuellen Bearbeitung einbezogen werden sollten, falls die Daten vorgehend oder nachfolgend in einem automationsunterstützten Vorgang verarbeitet werden. Konkret heisst das, dass von den Bearbeitungshandlungen schon das manuelle Ausfüllen eines Formulars in den Anwendungsbereich des Gesetzes fällt, falls diesem Vorgang später eine auch nur in einer Beziehung eine automationsunterstützte Nutzungsphase folgt (z.B. automatisches Erfassen der Formulare mit optischen Lesern [Scanner] und Speicherung auf Disks).

In einem künftigen schweizerischen Datenschutzgesetz sollte m.E. der Schutz der personenbezogenen Daten nicht allein auf die automatisierten Verarbeitungsvorgänge beschränkt bleiben. Es müsste zumindest eine Erweiterung auf die manuellen Verfahren aufweisen, die zum Zweck einer Ueberführung, als Vorbereitungs-, Zwischen- oder Nachfolgevorgang mit automatisierten Verarbeitungsschritten vorgenommen werden und eine Teilphase der ADV bzw. des gesamten mit automationsunterstützten Mitteln durchgeführten Verarbeitungsprozesses bilden.

besonderen Gefährdungen zugeschnittene Regelung verlangen und für die rein manuellen Verfahren - bei der Umstellung auf eine gesetzeskonforme Verarbeitung - eine zu grosse Belastung bedeuten könnte.

III. Materiell- und formellrechtliche Ausgestaltung des grenzüberschreitenden Datenverkehrs

Die nachfolgenden Ausführungen bezwecken nicht die Darstellung eines bis ins kleinste Detail ausgearbeiteten Lösungsmodells zum grenzüberschreitenden Datenverkehr, sondern erstellen einen Raster eines denkbaren Konzepts, ohne auf Einzelheiten näher einzutreten.

Dabei ist der Aufriss dieses Konzepts für den privaten Bereich gedacht, da dieser einerseits das grössere Volumen im grenzüberschreitenden Verkehr einnimmt und andererseits z.T. weitergehender Bestimmungen bedarf als der vom Legalitätsprinzip beherrschte öffentliche Sektor. Zweifelsohne sollte der öffentliche Bereich von den Grundideen des privaten Bereiches inspiriert und von ihnen, soweit möglich, in analoger Weise zu einem entsprechenden Konzept verarbeitet werden.

1. Notwendigkeit einer speziellen Regelung des grenzüberschreitenden Datenverkehrs in einem nationalen Gesetz

Die Notwendigkeit einer speziellen rechtlichen Ausgestaltung des grenzüberschreitenden Datenverkehrs im nationalen Datenschutzrecht folgt nicht alleine aus dem in § 1⁵⁸ nachgewiesenen Informationsaustausch, sondern auch aus der Zielfunktion des Datenschutzes im internationalen Rahmen sowie aus dem Regelungsbedarf der Verarbeitungsprinzipien und den Anforderungen an deren Qualität.⁵⁹

2. Differenzierung der rechtlichen Ausgestaltung im privaten Sektor

Die Ausgestaltung des grenzüberschreitenden Datenverkehrs bedarf einer Differenzierung hinsichtlich der am transnationalen Fluss beteiligten Datenverarbeitungsträger und ihren Verarbeitungszwecken: Sie darf aber nicht soweit gehen, dass eine rechtliche Spaltung inner-

58 Vgl. vorne, S. 1ff.

59 Vgl. vorne, S. 331ff.

halb der Regelung des grenzüberschreitenden Datenverkehrs im privaten Bereiches eintritt, es sind vielmehr Erleichterungen und Präzisierungen denkbar. Dabei ist von Wichtigkeit, dass jeder Transfer von personenbezogenen Daten mit dem Ausland als grenzüberschreitender Datenverkehr qualifiziert wird und nicht Begriffe (wie z.B. "Uebermitteln") oder rechtliche Qualifikationen (wie z.B. Haupt- und unselbständige Niederlassung) der am Austausch beteiligten Personen, die in verschiedenen Ländern gelegen sind, Ausnahmen zulassen.

A. Datenverkehr zwischen verschiedenen unabhängigen Stellen

Der grenzüberschreitende Datenverkehr zwischen verschiedenen, voneinander unabhängigen Gesellschaften bzw. verantwortlichen Stellen bildet den Normalfall und bedarf keiner besonderen Vorschriften. Hier haben i.d.R. die Prinzipien des Wettbewerbs, des geschäftlichen Geheimbereichs, der Vertragsverhältnisse usw. auf den Umfang des Datentransfers einen einschränkenden und steuernden Einfluss, der dem Datensubjekt eine gewisse Gewähr bietet, dass seine personenbezogenen Angaben im internationalen Bereich nicht von einer Stelle an die andere weiterverschoben werden, sondern nur im Rahmen der Zweckverwendung, deren sich das Datensubjekt meistens bewusst ist,⁶⁰ ins Ausland wandern.⁶¹

B. Datenverkehr innerhalb von multinationalen Gesellschaften

Der transnationale personenbezogene Informationsaustausch zwischen Mutter- und Tochtergesellschaften oder der letzteren untereinander ist nicht den gleichen Verletzungsrisiken ausgesetzt wie zwischen unabhängigen Gesellschaften, da die Daten immer innerhalb der gleichen Gesellschaft (nur im wirtschaftlichen Sinne) verbleiben.⁶² Die multinationalen Firmen bzw. deren Niederlassungen in den einzelnen Ländern verfolgen auch meistens den gleichen Geschäftszweck und sind

60 Z.B. bei Vornahme einer Flugreservation, weiss man, dass die Daten ins Ausland gelangen und dort auch verarbeitet werden; ebenso sind sich die Vertragspartner, die sich eines Akkreditives bedienen, bewusst, dass ihre personenbezogenen Angaben in Ausland gelangen.

ausserdem bestrebt, dass aus Gründen der Sicherheit und Vertraulichkeit die innerhalb des Unternehmens bearbeiteten Daten nicht an Dritte ausserhalb der Gesellschaft gelangen.

Diese Bestrebungen nach Schutz ihrer eigenen Informationen resultieren denn meistens in einem umfassenden Datenspeicherungskonzept innerhalb der ganzen Gesellschaft.⁶³ Der weltweit identische Geschäftszweck und die vorhandenen internen Sicherheitsmassnahmen sind eine erhöhte Gewähr für den Schutz der Daten im grenzüberschreitenden Fluss, so dass u.U. erleichterte Voraussetzungen zugelassen werden können.⁶⁴

Eine Ausnahme bilden die Fälle von multinationalen Unternehmen, die mehrere Gesellschaften, die in den verschiedensten Bereichen⁶⁵ tätig sind, beherrschen und die DV auch dazu benützen, gegenseitig personenbezogene Informationen auszutauschen: Sie müssten eine dem Normalfall des grenzüberschreitenden Datenverkehrs zwischen verschiedenen, voneinander unabhängigen Gesellschaften entsprechende Behandlung erfahren.⁶⁶

-
- 61 Einen Spezialfall bildet die Weitergabe eines bestimmten Interessenverbandes an eine zentrale Stelle wie z.B. die Weitergabe medizinischer Angaben, Gutachten und Lebensdaten durch amerikanische und kanadische Versicherungsgesellschaften an das Medical Information Bureau in Boston (USA), das einem Gesuchsteller erschwert, einen neuen Lebensversicherungsvertrag abzuschliessen, wenn er eine ungünstige medizinische Vorgeschichte aufweist (CARROLL, OECD Informatics Studies 10, S. 204 und andere Bsp.) - diese Fälle bedürften u.U. eines Hinweises auf die Speicherung im Ausland oder einer Spezialregelung.
- 62 Darunter fällt auch der Datenverkehr zwischen einer Hauptniederlassung im Inland und einer unselbstständigen Zweigstelle im Ausland oder umgekehrt.
- 63 Vgl. IBM Datenetze, vorne, S. 97.
- 64 Z.B. Erteilung einer Konzession für die Uebermittlung der Daten an andere Tochtergesellschaften oder Muttergesellschaft.
- 65 Z.B. Elektronikbranche, Hotelbranche und Flugsektor etc.
- 66 Vgl. A., vorne, S. 352.

C. Datenverkehr zwischen Stellen, die im Auftrag für Dritte Daten verarbeiten

Im Falle der Service-Rechenzentren, die im Auftrage von Dritten Daten verarbeiten und diese ins Ausland übermitteln, gilt es einen speziellen Punkt zu berücksichtigen.

Rechenzentren haben die Möglichkeit, die personenbezogenen Daten, zu deren Verarbeitung sie ein Auftraggeber ermächtigt hat, an ausländische Stellen zu übermitteln und sie dort verarbeiten zu lassen, z.B. um die günstigere Kostenstruktur in einem Billig-Lohn-Land auszunutzen. M.E. sollte hinsichtlich eines solchen Exportes noch als zusätzliches Erfordernis aufgestellt werden, dass der Auftraggeber über die aus ökonomischen Gründen im Ausland erfolgende Datenverarbeitung zu informieren ist. Es erscheint mir im Rahmen des Vertrauensprinzips untragbar, wenn beim Abschluss eines Rechenzentrumsvertrages der Auftraggeber keine Kenntnis von der auswärtigen Verarbeitung hat,⁶⁷ gleichgültig, ob der Auftraggeber oder das Rechenzentrum vom nationalen Recht als verantwortliche Stelle deklariert wird. Hier ist deshalb eine ausdrückliche Zustimmung des Auftraggebers zur Verarbeitung der Daten im Ausland zu fordern. M.a.W. eine Informationspflicht des Rechenzentrums gegenüber dem Auftraggeber erscheint unerlässlich. Damit wird letzterem auch die Wahl offen gehalten, Trivialdaten in einem ausländischen Billig-Lohn-Staat verarbeiten zu lassen, personenbezogene sowie sensitive Informationen dagegen, der höheren Sicherheit wegen, nur im Inland.

67 FREESE (Data Flow, S. 30) stellt fest, dass eine grosse Zahl von Unternehmen, die Rechenzentren benutzen, vielfach nicht wissen, wo die Daten verarbeitet werden.

68 Nicht speziell erwähnt wird, dass aufgrund des komplementären Charakters von Export und Import, d.h. dem Uebermitteln des Exporteurs, auf der Seite des Empfängers folgerichtig die Befugnis zum Ermitteln der Daten entspricht, und dieser (der Importierende) über eine solche verfügen muss. Damit wird gleichzeitig für den Ausführenden das Risiko eines nicht gesetzlich erfassbaren Missbrauchs im Ausland eliminiert (vgl. STADLER, Datenschutzrecht, S. 64).

3. Ausfuhr personenbezogener Daten

A. Voraussetzungen ⁶⁸

a) Formelle

- aa) Prinzip: Registrierungspflicht für den privaten Sektor ⁶⁹ vor
Aufnahme des grenzüberschreitenden Datenverkehrs. ⁷⁰

Unabhängig davon, ob man im (künftigen schweizerischen) Datenschutzrecht für den privaten Bereich die generelle Zulässigkeit der Datenverarbeitung von einer Deklaration, Registrierung oder Bewilligung abhängig macht oder sie formfrei gestaltet, erachte ich eine Registrierung dann als sinnvoll, wenn eine verantwortliche Stelle grenzüberschreitenden Verkehr personenbezogener Daten unterhält, d.h. Daten exportiert oder importiert werden. Die Registrierung sollte dabei nicht bloss formelle oder deklarative Bedeutung haben, sondern von einer vorgängigen Ueberprüfung der Datensicherungsvorkehrungen- und -einrichtungen ⁷¹ abhängen, denen im internationalen Austausch ein bedeutender Stellenwert der Schutzwirkung zukommt. Es sind grundsätzlich weitere Voraussetzungen denkbar, die für eine Registrierung notwendig sein können. Die Registrierung darf jedoch nicht zu einem versteckten Hindernis für den grenzüberschreitenden Datenverkehr werden, sondern muss in ihren Voraussetzungen so ausgestaltet sein, dass dieser Formalakt sowohl im Rahmen eines internationalen Rechtsregimes, das einen genehmigungsfreien grenzüberschreitenden Datenfluss statuiert, als auch ausserhalb eines vertraglichen Schutzgebietes zwischen Staaten mit und ohne Datenschutzgesetzgebung auf seine Schutzfunktion beschränkt bleibt. Die Registrierung hat in diesem Lösungsmodell den Eintrag in einem Datenverarbeitungsregister zur Folge, das eine erhöhte Transparenz im Bereich des grenzüberschreitenden Datenverkehrs bezweckt. Der Registereintrag darf aber im privaten

69 Im öffentlichen Bereich ist m.E. eine generelle Registrierungs-
pflicht aus Gründen der Transparenz der DV in der öffentlichen
Verwaltung notwendig.

70 Ähnlich dem Vorbild des österreichischen Gesetzes.

71 Z.B. Zurückbehalten einer Kopie der übermittelten Daten.

Bereich keinen derart hohen Detaillierungsgrad aufweisen,⁷² dass dabei das im privatwirtschaftlichen Bereich existierende grundsätzliche Bedürfnis auf Geheimhaltung der wirtschaftlichen und geschäftlichen Information⁷³ durch eine Offenlegung der Tätigkeit im grenzüberschreitenden Datenverkehr verletzt wird. Die Wettbewerbsneutralität des Datenschutzes muss als Abgrenzungskriterium dafür dienen, dass durch die Forderung nach Transparenz nicht die Geheimhaltung der wirtschaftlichen Sphäre verletzt wird. Der Registereintrag sollte aber auch Ausdruck der Garantie sein, dass die für den transnationalen Verkehr erforderlichen Sicherungsmassnahmen erfüllt sind.

bb) Zweck

Der Zweck dieses Registereintrages besteht darin, jedem zum Export befähigten Datenverarbeiter eine Registernummer und einen Landescode zuzuordnen, die bei der Uebermittlung der Daten ins Ausland dem Datensatz beigefügt werden müssen.⁷⁴ Damit ist für eine ausländische Stelle, die von mehreren Datenverarbeitern personenbezogene Informationen erhält, jederzeit deren Ursprung bzw. Ursprungsland⁷⁵ feststellbar. Es bleibt dem Urteil der Gesetzgebers überlassen, ob

-
- 72 Im öffentlichen Bereich gilt der umgekehrte Ansatz: Grundsätzlich hoher Detaillierungsgrad über Herkunft, Art, Zweckverwendung, Uebermittlungsgrund, Empfänger etc. der Daten; diese weitgehende Transparenz erfährt eine Einschränkung durch höherwertige Interessen, die ihr prinzipiell entgegenstehen, wie z.B. nationale oder öffentliche Sicherheit, Landesverteidigung etc. Im privaten Bereich ist grundsätzlich von der Geheimsphäre des Unternehmens auszugehen, die eine umfassende Transparenz über die Datenbestände, ihre Herkunft, Verwendungsart, Uebermittlungszweck, Empfänger, Datenflüsse etc. verbietet. Dieser Grundsatz wird nur durchbrochen, wenn Datensammlungen oder DV-Prozesse Daten enthalten, die besonders stark in Persönlichkeitsrechte eingreifen wie z.B. medizinische Daten, sensitive Informationen. Bei diesen Datenkategorien ist (je nach Benutzer und Zweckverwendung) eine erhöhte Transparenz zu fordern.
- 73 Als Ausdruck des Geschäfts- und Unternehmensgeheimnisses.
- 74 Prinzip eines "DV-Indossamentes", das jederzeit den Ursprung des Datums bzw. Datensatzes sowie die Zwischenstufen der Uebermittlung und Verarbeitung erkennen lässt.

ein solches "DV-Indossament" nicht auch bei den Uebermittlungen im nationalen Bereich vorgesehen werden sollte, was allerdings die allgemeine Deklarationspflicht jeder DV-Tätigkeit und einen Registereintrag zur Erteilung einer Registernummer voraussetzen würde.

Die Identifikation des Ursprungslandes eines Datums spielt m.E. im internationalen Kontext eine bedeutende Rolle, vor allem dann, wenn es um die Frage eines Wiederexportes geht. Die Bedeutung des Ursprungsprinzips ist vor allem im Rahmen eines vertraglich vereinbarten Schutzraumes (Konvention) hervorstechend, weil es eine einfache und klare Lösung zum Problem des Wiederexportes von Daten aus Konventionsstaaten an Drittländer bietet.⁷⁶

Es wäre zu überdenken, ob nicht die exportierende Stelle auch verpflichtet werden sollte,⁷⁷ eine Kopie des übermittelten Datenbestandes aufzubewahren.⁷⁸ In der Praxis kommt dies häufig nicht allein aus verarbeitungstechnischen Gründen vor, weil die Daten weiteren Verarbeitungsschritten unterzogen werden und nur eine Kopie ins Ausland transferiert wurde (z.B. zu Konsolidierungszwecken), sondern auch zur Datensicherung, wenn eine Spezialverarbeitung im Ausland vorgenommen wurde. M.E. ist auch denkbar, dass die Datenausfuhr nur dokumentiert wird, d.h. eine Aufzeichnung erfolgt, welche Datenbestände an welche Empfänger gehen bzw. welche ausländischen Stellen auf welche Datenarten über Terminal Zugriff haben.

Aus dem Festhalten des Ursprungslandes bzw. Erstexporteurs könnten auch spätere Anfragen zwecks Nachführungen, Berichtigungen oder Ergänzungen erleichtert werden, da die exportierende Stelle i.d.R. auch ein Interesse an der Richtigkeit der Daten hat, so dass das Ursprungsprinzip mit ein Beitrag zur Erhöhung der Datenqualität sein kann.

75 I.d.R. ist der Wohnsitzstaat einer Person zugleich Ursprungsland der Daten, weil die meisten Informationen am Wohnsitzort gesammelt werden. Das Recht des Ursprungsortes hat somit meistens auch die engste Beziehung zum Datensubjekt, weil es gleichzeitig das Wohnsitzrecht ist.

76 Vgl. vorne, S. 322.

77 Z.B. durch Datensicherungsmaßnahmen.

b) Materielle

Es stellt sich die Frage, ob ein nationales Gesetz als materielle Voraussetzung den Schutz der exportierten Daten im Importland fordern kann und soll. M.E. ist dies zu bejahen und in Abhängigkeit von der formellen Ausgestaltung der Exportregelung entsprechend vorzunehmen:

- Wird ein genehmigungsfreies System ⁷⁹ zugrundegelegt, ist es sinnvoll, die Befugnis zum Export von einem wirksamen Schutz der Daten im Destinationsland abhängig zu machen. Dies bedeutet die Aufnahme einer materiellen Bestimmung in die Regelung, die eine solche Voraussetzung schafft, da sonst das nationale Gesetz keinen wirksamen Schutz der Daten im Ausland realisieren wird.
- Beim Genehmigungssystem ⁸⁰ erübrigt sich eine solche Voraussetzung, weil durch das Instrument der Genehmigung vor der Ausfuhr bzw. jederzeit überprüfbar ist, ob im Empfängerland ausreichende Schutzmassnahmen existieren oder nicht.

Die Anwendung der verschiedenen Ausprägungen des Genehmigungssystems (Konzession, Muster- und Einzelgenehmigung) sollte aber nicht alleine dem Ermessen der die Genehmigung erteilenden Kommission überlassen werden, sondern durch gesetzliche Grundregeln und Orientierungsbestimmungen so gestaltet sein, dass eine Beurteilbarkeit und Vorhersehbarkeit der anzuwendenden Norm bzw. Genehmigungsstufe aufgrund der konkreten Sachlage möglich ist. Dies verhindert behördliche Willkürakte und erhöht die Rechtssicherheit für in- und ausländische Stellen.

B. Grundsatz: Exportregelung ohne Berücksichtigung einer internationalen Vereinbarung.

Gegenüber dem Ausland, d.h. den Staaten mit oder ohne Datenschutzgesetzgebung, ist das Genehmigungssystem ⁸¹ das geeignete In-

78 Aufbewahrung bis zum Wiederimport oder nur für bestimmten Zeitraum.

79 Vgl. vorne, Nr. 4, S. 234ff.

80 Vgl. vorne, Nr. 2, B., S. 224ff.

strument,⁸² um eine flexible und einfache Gestaltung des Exportes sowie einen optimalen Schutz dieser Daten im Ausland zu erreichen. Der Vorteil des Genehmigungssystems liegt darin, dass es nicht nur für den Grundsatz, d.h. den Normalfall, eine Lösung bietet, sondern auch den Ausnahmefall⁸³ abdeckt.

Zugunsten einer datenverarbeitungsfreundlichen Regelung kann dabei noch unterschieden werden zwischen dem erstmaligen bzw. wiederholten Exporten, d.h. der Ausfuhr von Ursprungsdaten und der Wiederausfuhr importierter personenbezogener Daten.

a) Export von Ursprungsdaten

Der Export personenbezogener Daten, die im Inland gesammelt, erfasst, verarbeitet, gespeichert und/oder anderen Verarbeitungsschritten unterzogen und ins Ausland übertragen werden, verkörpert den Normalfall. Es handelt sich um die Ausfuhr von Daten, die ihren Ursprung im nationalen Territorium haben und damit unter einen anderen gesetzlichen Schutzbereich treten.

Für die Ausfuhr dieser Daten kann mit den Abstufungen des Genehmigungssystems leicht auf die unterschiedlichen Schutzbedürfnisse der personenbezogenen Informationen gegenüber einzelnen Ländern reagiert werden:

- Die Einzelgenehmigung⁸⁴ kann für eine einmalige Ausfuhr von bestimmten Datenarten an einen genau festgelegten Empfänger ausgesprochen werden. Sie ist überall dort angebracht, wo die besonderen Umstände des Destinationslandes eine restriktive Genehmigungserteilung nach individueller Prüfung des Einzelfalles wegen fehlenden oder unvollständigen Schutz rechtfertigen.
- Eine Mustergenehmigung⁸⁵ ist auf diejenigen Exportfälle zugeschnitten, bei denen eine verantwortliche Stelle einen mehrfachen

81 Vgl. vorne, Nr. 2, S. 224ff.

82 Vgl. auch 2. Tätigkeitsbericht d.B.f.D., Nr. 4.3.8, S. 67.

83 Annahme: Export mit Berücksichtigung eines internationalen Rechtsregimes, vgl. hinten C., S. 364ff.

84 Vgl. vorne, S. 224ff.

85 Vgl. vorne, S. 226ff.

Export bestimmter Datenarten an einen genau fixierten Empfänger oder Empfängerkreis in einem oder mehreren bezeichneten Staaten vornehmen muss. Sie eignet sich z.B. für den Export in Staaten, die ein weitmaschiges Datenschutzrecht oder keine Datenschutzgesetzgebung bzw. -normen haben, deren Rechtsordnung aber ein bestimmtes Mass an Persönlichkeitsschutz aufweist und die Empfänger auch keine besondere Gefahr für eine missbräuchliche Verwendung darstellen.

- Die Konzession ⁸⁶ schliesslich ermöglicht einem bestimmten Datenverarbeiter den mehrfachen Export verschiedene Kategorien von personenbezogenen Daten an einen genau bezeichneten Kreis von Empfängern in verschiedenen Ländern. Die Konzession ist die typische Genehmigungsart für multinationale Gesellschaften, die intern einen hohen Schutzstandard entwickelt haben und auf einen möglichst ungehinderten Datenfluss mit den andern Gesellschaftstöchtern sowie dem Mutterhaus angewiesen sind, ohne dass auf das Vorhandensein einer Datenschutzgesetzgebung in einem Niederlassungsland geachtet wird. Eine Konzession kann auch befristet erteilt werden.
- Ein Verzicht auf das Erfordernis einer Exportbewilligung ⁸⁷ ist in all jenen Fällen angezeigt, bei denen Daten an einen oder mehrere Destinatäre in einem Lande gelangen, das den übermittelten Datenarten einen mit dem Inland vergleichbaren Schutz zukommen lässt.

Der beschränkt freie Datenexport ist somit grundsätzlich gegenüber allen datenschutzbewussten Nationen zu pflegen, die einen vergleichbaren, d.h. zumindest gleichwertigen oder weitergehenden Schutz vermitteln. Gegenüber Staaten, die eine weniger weitgehende Schutzwirkung realisiert haben, müssen die verschiedenen Genehmigungsstufen (Konzession, Muster- und Einzelgenehmigung) zum Einsatz kommen. Welche Datenschutzstaaten ein mit dem Inland vergleichbares Schutzniveau aufweisen können, muss in geeigneter Form von der die

86 Vgl. vorne, S. 228ff.

87 Vgl. vorne, S. 231 und ff.

Genehmigung erteilenden Behörde (Datenschutzbehörde) bekanntgegeben werden. I.d.R. klärt sich diese Frage beim Einholen einer Genehmigung, d.h. im Zweifel ist eine Genehmigung zu beantragen.

Zusammenfassend kann somit unterschieden werden zwischen Genehmigungsformen für den Export in Staaten mit einer dem Inland vergleichbaren Datenschutzgesetzgebung und in solche mit einer gegenüber dem inländischen Schutz zurückstehenden Wirkung.

Für die gesetzliche Regelung des Exportes in Länder ohne vergleichbare Datenschutzgesetzgebung werden die Genehmigungsstufen der Konzession, Muster- und Einzelgenehmigung Exportfälle vorgeschlagen, hingegen kann der Datenexport in Länder, die den Daten eine dem Inland vergleichbare Schutzwirkung vermitteln, genehmigungsfrei erfolgen. Dieses Modell bietet den Vorteil, dass es den datenverarbeitenden Stellen bis zum Zeitpunkt der Verbindlichkeit einer internationalen Vereinbarung den genehmigungsfreien Austausch ermöglicht und gleichzeitig die Schutzwirkung der Daten im Ausland garantiert bleibt.

Es bleibt der Ausnahmefall zu überlegen, ob es sinnvoll ist, auf eine Genehmigung grundsätzlich zu verzichten, wenn das Datensubjekt seine schriftliche Einwilligung zum Export der Daten gegeben hat. Dies müsste im Rahmen des informationellen Selbstbestimmungsrechtes möglich sein - es wären immerhin Bestimmungen zu erlassen, die vorschreiben, dass ein in Erhebungsformularen vorhandener Hinweis auf die im Ausland erfolgende Verarbeitung dem Datensubjekt deutlich zur Kenntnis gelangt.

Zum Problem der Regelung des Weiterexportes der mit oder ohne Genehmigung in andere Länder exportierten Daten sind zwei Lösungen denkbar:

- Die entsprechende Genehmigungsform wird dem Gestaltsteller nur erteilt, falls sich der ausländische Empfänger verpflichtet, die übermittelten Daten nicht in einen Drittstaat zu exportieren.
- Die Gefahr des Weiterexportes durch den ausländischen Empfänger wird bei der Beurteilung des Bewilligungsgesuches berücksichtigt; u.U. sind spezielle Auflagen an die exportierende Stelle denkbar.

b) Wiederexport von importierten Daten

Diese Unterscheidung ist im Interesse eines möglichst freien internationalen Datenflusses ohne entsprechenden multilateralen Vertrag gegeben. Es gilt, den einheimischen Datenverarbeitern eine Kapazitätsausschöpfung der im Inland installierten DV-Systeme und Programme durch Benützer im Ausland zu ermöglichen, ohne dabei den importierten Daten den inländischen Schutz vorzuenthalten.

Eine nationale Norm müsste daher eine Ausnahmeregelung von der Genehmigungspflicht zum Export für solchermaßen importierte Daten vorsehen. Dabei ist einziges Erfordernis, dass die importierten Daten bei ihrer Verarbeitung im Inland keine Verknüpfung oder Vermischung mit Daten des Inlands, sog. Ursprungsdaten, erfahren. Ist von der verantwortlichen Stelle im Inland sichergestellt, dass keine weiteren Verarbeitungshandlungen erfolgt sind, muss die Wiederausfuhr ohne die Einholung einer speziellen Genehmigung möglich sein;⁸⁸ wurden hingegen dem importierten Datenbestand auch Informationen aus einheimischen Datensammlungen beigefügt, ist der Export nach dem Genehmigungssystem zu beurteilen, d.h. gleich zu behandeln wie Daten, die ihren Ursprung im Inland haben.

Für den Spezialfall, dass im internationalen Datenverkehr ausländische Stellen den Export in die Schweiz dazu vornehmen, um unser Land als Transitstaat bzw. Transitverarbeitungsland für eine Gesetzesumgehung zu benutzen, und zu diesen Zwecken Daten importiert und wieder ausgeführt werden, wäre u.U. ein Exportverbot bei entsprechendem Ersuchen eines andern Datenschutzstaates als Ausnahme angebracht und vorzusehen.

c) Zugriff auf inländische Datenbanken

Da der Zugriff auf inländische Datenbanken durch Stellen im Ausland ebenfalls unter dem Export einzureihen und keine rechtliche

⁸⁸ Vgl. Regelung in Dänemark, Gesetz für private Register: § 21 Abs. 2 Satz 3, vgl. vorne, S. 204.

Sonderbehandlung angezeigt ist,⁸⁹ muss das Genehmigungssystem auch auf diese spezielle Erscheinungsform des grenzüberschreitenden Datenverkehrs anwendbar sein.

Bei Betrachtung der am Austausch beteiligten Parteien ist eine Lösung insofern denkbar, als der ausländische "Benützer" mit der für die Datenbank verantwortlichen Stelle einen speziellen Vertrag abschliessen muss, in dem der Benützer das Vorhandensein spezieller Schutzvorkehrungen nachweist⁹⁰ und sich zur Beachtung besonderer Schutzvorschriften verpflichtet. Aufgrund dieses "Zugriffsvertrages" wird der verantwortlichen Stelle im Inland eine Genehmigung erteilt, die sie ermächtigt, dem im Ausland befindlichen Empfänger das vertraglich vereinbarte Zugriffsrecht nach erfolgter Vornahme der Sicherheitsvorkehrungen (z.B. Verschlüsselung von exportierten Daten) einzuräumen. Im Falle einer Persönlichkeitsverletzung wären sowohl die verantwortliche Stelle im Inland als auch der ausländische Benützer zivilrechtlich solidarisch haftbar.

Es versteht sich, dass diese Genehmigung nur gegenüber Staaten⁹¹ notwendig ist, die keine vergleichbare Datenschutzgesetzgebung erlassen haben. Zwischen Staaten mit einem vergleichbaren Schutzniveau bzw. Gesetzgebung ist analog zum Normalfall des Exportes keine Genehmigung erforderlich.

Auch hier erweist sich das Genehmigungssystem als tauglich für eine einfache Lösung und abgestuftes Lösungsschema.

89 Vgl. vorne, S. 287f.

90 Nachweis oder Bestätigung der einheimischen Datenschutzbehörde seines Sitzlandes.

91 Staat, in dem sich die technischen Einrichtungen (z.B. Terminal) befinden, die einen Zugriff auf Datenbanken ermöglichen.

C. Ausnahme: Exportregelung im Hinblick auf internationale völkerrechtliche Vereinbarungen (z.B. Konvention)

Ein nationaler Gesetzgeber, der sich anfangs der 80er Jahre mit der Ausarbeitung eines Datenschutzgesetzes befasst, darf die aktuellen Bemühungen internationaler völkerrechtlicher Vereinbarungen über den transnationalen Datenverkehr nicht unberücksichtigt lassen. Da diese Bestrebungen auf die Errichtung eines internationalen Rechtsregimes⁹² zielen, sollte ein Datenschutzgesetz aus dieser Dekade auch einen von Bewilligungen und Genehmigungsschranken möglichst freien Verkehr zwischen den einer internationalen Vereinbarung angeschlossenen Staaten vorsehen.

a) Fall des Exportes in Mitgliedstaaten der Konvention

Um einen freien Datenfluss zu gewährleisten, sollte das Gesetz auf die Einholung einer Genehmigung und anderer den freien Verkehr hindernden Bestimmungen grundsätzlich verzichten, falls eine völkerrechtliche Vereinbarung zum Schutz der Persönlichkeit im grenzüberschreitenden Datenverkehr einen freien Informationsaustausch aller Arten von Daten (auch personenbezogener) vorsieht. Innerhalb eines Genehmigungssystems könnte somit die freie Ausfuhr i.S. des beschränkt freien Datenexportes⁹³ für das Territorium der der Vereinbarung beigetretenen Länder ausgesprochen werden.⁹⁴

Ausnahmefälle, die zu einem Exportverbot führen, sind auch hier denkbar.

92 STADLER, OeVD 1-2/79, S. 4; ders. DS + DS 3/79, S. 173; FREESE, Data Flow, S. 8.

93 Vgl. vorne, S. 231ff.

94 Vgl. auch österreichische Regelung, § 32 Abs. 2 Ziff. 3 DSG.

b) Fall des Wiederexportes an Drittstaaten

M.E. muss die nationale Exportregelung im Hinblick auf ein internationales Rechtsregime u.U.⁹⁵ auch den Fall des Wiederexportes von Daten, die aus einem Vertragsstaat des geschützten Raumes stammen, vorsehen.

Für die Wiederausfuhr der aus dem Vertragsgebiet stammenden Daten sind mehrere Regelungsformen möglich. Hauptzweck dieser Norm ist zu verhindern, dass die eigene Gesetzgebung ein Wegfliessen von Daten in Drittstaaten ermöglicht, da dies eine Schwächung des geschützten Gebietes bedeuten würde und mit Sperrmassnahmen durch die übrigen Mitgliedstaaten beantwortet werden könnte. Eine Regelung muss nicht nur geeignet sein, das Vertrauen der andern Mitgliedsländer in die Wirksamkeit des schweizerischen Datenschutzrechts zu stärken, sondern durch diese erhöhte Sicherheit indirekt auch den datenverarbeitenden Wirtschaftszweigen eine ökonomisch günstige Ausgangslage zu schaffen.⁹⁶

Die restriktivste Schutzmethode wäre eine Regelung, die den Wiederexport eines Datums grundsätzlich verbietet und die Ermächtigung dazu allein dem Ursprungsland⁹⁷ erteilt. Es ist aber auch denkbar, für einen Wiederexport sowohl die Zustimmung der Behörde des Ursprungslandes als auch des Inlandes zu fordern.

Die unterste Stufe einer restriktiven Regelung ist erreicht, wenn der Wiederexport dem Normalfall gleichgestellt, d.h. nach dem Grundsatz des Exportes ohne Berücksichtigung einer internationalen Konvention beurteilt wird; als zusätzlich erschwerendes Erfordernis ist ein von der ausführenden Stelle zu leistender Nachweis denkbar, der klarlegt, dass die beabsichtigte Ausfuhr keine Gesetzesumgehung gegenüber dem Recht des Ursprungslandes darstellt; es könnte aber

95 D.h. falls das internationale Rechtsregime darüber nichts aussagt; die nationale Gesetzgebung müsste eine Regelung unter dem Vorbehalt einer abweichenden Normierung durch die internationale Vereinbarung erlassen.

96 Vgl. Auswirkungen des Bankgeheimnisses.

97 Dabei müsste aber als formale Voraussetzung sichergestellt sein, dass das Ursprungsland eines Datums leicht auszumachen bzw. festzustellen ist.

auch der Vorbehalt einer Einrede durch einen andern Vertragsstaat vorgesehen werden.

Nur mit einer sehr einschränkenden Regelungsart ist die Entstehung von data havens zu verhindern.

4. Einfuhr personenbezogener Daten

A. Voraussetzungen

Wie vorgehend ⁹⁸ ausgeführt, ist die formelle Voraussetzung der Registrierung grundsätzlich vor der Vornahme des grenzüberschreitenden Datenverkehrs zu erfüllen, somit auch vor einem Import von Daten. Aus der Gleichbehandlung der den grenzüberschreitenden Datenverkehr betreibenden Stellen folgt, dass auch der Importeur eines Eintrages im Datenverarbeitungsregister bedarf und mögliche weitere Voraussetzungen erfüllen muss (z.B. Deklaration, Protokollierung der Import/Exportvorgänge, der Herkunft und des Bestimmungsortes der Daten usw.).

B) Grundsatz: Importregelung ohne Berücksichtigung einer internationalen Vereinbarung

Der Import kann grundsätzlich wie die Ausfuhr nach den Prinzipien des Genehmigungssystems geregelt werden, wobei aber hier der besondere Umstand berücksichtigt werden muss, dass die Daten in den Anwendungsbereich des inländischen Rechts treten. Das Genehmigungssystem folgt dabei in analoger Weise dem beim Export ⁹⁹ beschriebenen Muster, so dass auf eine nähere Erläuterung verzichtet werden kann.

a) Import von Daten ausländischen Ursprungs

Auf eingeführte Daten, die ihren Ursprung im Ausland haben, soll grundsätzlich das inländische Recht anwendbar sein - dies folgt aus dem Prinzip der Gleichbehandlung.

98 Vgl. vorne, 3.,A.,a), S. 355.

99 Vgl. vorne, 3.,B., S. 358.

Für die Einfuhr solcher Daten ist m.E. grundsätzlich von einer Genehmigung abzusehen, da sie ja in den Anwendungs- und Schutzbereich des inländischen Datenschutzrechts treten. Mit dieser genehmigungsfreien Einfuhr ist aber nicht ein freier Import schlechthin gemeint, sondern die beschränkt freie Einfuhr,¹⁰⁰ die jederzeit unterbunden und einer Konzession-, Muster- oder Einzelgenehmigung unterworfen werden kann. Der Vorbehalt des Verbotes, welcher seinerseits wieder von den verschiedenen Genehmigungsstufen aufgehoben werden kann, ist für die Fälle vorgesehen, bei denen die Datenkategorien selbst oder die Art ihrer im Ausland erfolgten Verarbeitung eine Verletzung oder Umgehung des inländischen Rechts darstellen.

Das Bekenntnis zur grundsätzlich genehmigungsfreien Dateneinfuhr wird aber auch schon durch die beim Export postulierte erleichterte Wiederausfuhr von importierten personenbezogenen Informationen, die keine Vermischung mit Daten des Inlandes erfahren haben,¹⁰¹ konsequenterweise vorausgesetzt.

b) Wiederimport exportierter Daten

Sind Daten, die ihren Ursprung im Inland haben, in gesetzeskonformer Weise ausgeführt worden, stellt ihr Wiederimport keinerlei Probleme. Sie können aber auch im Ausland Verarbeitungsschritten oder -verfahren unterzogen worden sein, die im Inland nach der geltenden Rechtsordnung nicht erlaubt wären; in solchen Fällen muss der grundsätzlich genehmigungsfreie Wiederimport mittels eines Genehmigungsvorbehaltes beschränkt oder verhindert werden können.

c) Zugriff auf ausländische Datenbanken

Es ist denkbar, dass im Ausland Datenbanken aufgebaut werden, deren Errichtung und Unterhalt wegen besonderer Verarbeitungsvor-

100 Analog der Typisierung des beschränkt freien Exportes, vgl. vorne, S. 231ff.

101 Vgl. vorne, 3., B., b), S. 362.

gänge oder Einbeziehung sensibler Datenkategorien im Anwendungsbereich des nationalen Gesetzes nicht gestattet ist. Es wäre eine unvollkommene Ordnung, wenn das nationale Gesetz den Aufbau derartiger Datensammlungen im Inland zwar untersagt, diese Norm aber durch einen Zugriff auf im Ausland befindliche Datenbanken von einem im Inland gelegenen Terminal aus umgangen werden könnte.

Es bedarf keiner weiteren Erläuterungen, dass mit dem Normalfall des freien Importes - unter Vorbehalt eines Genehmigungssystems für besondere Tatbestände - einerseits der freie Datenverkehr gefördert werden kann, andererseits jedoch einer Verletzung oder Umgehung der nationalen Vorschriften mit einer geeigneten Abwehr begegnet werden kann.

Für alle Formen des Importes ist somit von der grundsätzlich genehmigungsfreien Einfuhr¹⁰² auszugehen. Droht in einzelnen Fällen durch den Import eine Persönlichkeitsverletzung oder führt er zu einer Verletzung der Rechtsordnung oder Umgehung von Schutznormen, ist das Genehmigungssystem das geeignete Mittel für eine individuelle Überprüfung des Falles durch eine abgestufte Ausnahmeregelung mit den verschiedenen Stufen der Konzession, Muster- und evtl. Einzelgenehmigung.

C. Ausnahme: Importregelung im Hinblick auf internationale völkerrechtliche Vereinbarungen

a) Grundsatz: Garantie des freien Datenimportes aus dem Vertragsgebiet

Im Hinblick auf eine internationale Vereinbarung,¹⁰³ deren Zweck nicht nur im Schutz der Daten auf internationaler Ebene, sondern auch in einem freien Informationsfluss besteht, müssen entsprechende Bestimmungen erlassen werden, die auf nationaler Ebene zur Unterstützung dieser Zielprojektion beitragen. Diese Zielsetzung

102 I.S. einer beschränkt freien Ausfuhr bzw. Einfuhr.

103 Vgl. vorne, S. 364.

sowie das Postulat des freien Exportes in Vertragsländer¹⁰⁴ be-
dingen als Korrelat einen genehmigungsfreien Import. Die bewilligungs-
freie Zulassung der Ausfuhr im internationalen Kontext kommt aber nur
zum Tragen, wenn auch ein Import im geschützten Konventionsgebiet als
genehmigungsfrei ausgestaltet ist.

b) Ausnahme: Genehmigung für Importe aus dem Konventionsgebiet

Der Grundatz des freien Importes darf aber nicht absolute Gel-
tung haben, sondern muss m.E. dort, wo die Genehmigungsfreiheit der
Einfuhr zur Verletzung von nationalen Rechtsvorschriften eines Mit-
gliedstaates führen, durchbrochen werden. Eine Regelung, welche die
Einfuhr einer Genehmigung unterstellt, falls erwiesen ist, dass der
Exporteur die Einfuhr und die Verarbeitung im Inland nur dazu be-
nutzt,¹⁰⁵ um bestehende restriktivere Bestimmungen des Ursprungs-
landes zu umgehen, wäre eine denkbare Lösung in diesem Konzept.

Der Vorbehalt der Importgenehmigung sollte nur aufgrund des Er-
suchens eines ausländischen Staates und nach einer Ueberprüfung der
Rechtmässigkeit ausgesprochen werden. Ein ausländisches Begehren er-
scheint notwendig, weil ohne diese Voraussetzung die nationalen Be-
hörden zu dauernden inquisitorischen Nachforschungen im privaten Be-
reich angehalten wären, was nicht praktikabel und nur schwer durch-
führbar wäre. Die Ueberprüfung der Rechtmässigkeit des Gesuches er-
scheint notwendig, um die importierenden und exportierenden Stellen
vor Willkür- und Störungsaktionen ausländischer Staaten im Interesse
des freien Datenflusses zu schützen.

Es versteht sich, dass diese Ausnahme nur als ultima ratio in
besonders krassen Fällen zur Anwendung kommen sollte. M.E. ist jedoch
ein Genehmigungsvorbehalt gegenüber dem garantierten freien Import
notwendig, um das Vertrauen in die Wirksamkeit des nationalen Daten-

104 Vgl. vorne, S. 364.

105 Z.B. zur erleichterten Wiederausfuhr an Drittstaaten, d.h. zur
Benutzung als Transitstaat oder Transitverarbeitungsstaat.

schutzrechtes gegenüber Mitgliedstaaten zu stärken.

Um die Anpassung einer derartigen Regelung auf die schnell fortschreitende Rechtsentwicklung zu gewährleisten, sollte ein Vorbehalt für eine abweichenden Regelung durch ein internationales Rechtsregime aufgenommen werden.

5. Transit

A. Sonderregelung für Transitdatenflüsse

Da im Rahmen des grenzüberschreitenden Datenverkehrs personenbezogene Informationen nicht nur aus- bzw. eingeführt werden, sondern auf den Medien der Fernmeldekommunikation nationales Territorium passieren, kann auch dieser Vorgang eine Quelle von Persönlichkeitsverletzungen darstellen. Wichtig ist, dass durch eine nationale Norm die internationalen Transitwege der Daten nicht behindert werden, sondern nur der Schutz dieser Wege vom Gesetz garantiert und die mit dem Funktionieren der Datennetze zusammenhängenden systemtechnischen Verarbeitungsvorgänge (z.B. Zwischenspeicherung) gegenüber den übrigen Bearbeitungen abgegrenzt werden.¹⁰⁷ Diese Ausklammerung würde bedeuten, dass alle mit dem Transit durch das Inland zusammenhängenden Verarbeitungsschritte, die von der Datennetzsteuerung der im Inland befindlichen DV-Systeme vorgenommen werden, nicht unter den Anwendungsbereich des nationalen Gesetzes fallen. Die Sonderregelung bezweckt, dass die internationalen Transitwege der Datennetze, die auf einem Zusammenwirken der Datenverarbeitung mit den Verfahren der Telekommunikation beruhen, nicht durch das nationale Gesetz behindert oder unterbrochen werden.

106 Transit bedeutet, dass die Daten den Rechtsbereich eines Landes nur passieren, während dieses Durchganges aber keinem Verarbeitungsvorgang unterzogen werden, der zu einer Mutation des Datenbestandes führen könnte.

107 Vgl. vorne, S. 337ff.

Ein Gesetz muss somit sicherstellen, dass die innerhalb eines geschlossenen Datennetzes oder öffentlichen Fernmeldeleitungen befindlichen personenbezogenen Informationen und die netzwerkbedingten Steuerungs- und Verarbeitungsvorgänge (wie z.B. das Zwischenspeichern), die von im Inland liegenden Maschinen- und/oder Programm-Komponenten ausgehen, nicht unter die allgemeinen Vorschriften des nationalen Gesetzes über die Verarbeitung von Daten subsumiert werden. Im Rahmen einer solchen Ausnahmeregelung müssten auch bestimmte Datenkategorien (z.B. sensitive Daten), deren Verarbeitung im Inland untersagt oder nur mit Einschränkungen erlaubt ist, auf ihrem Transit und bei transitbedingten Verarbeitungen von den allgemeinen nationalen Vorschriften des einheimischen Rechtsbereiches unberührt bleiben.

Diese Sonderregelung ist nur für den ausschliesslichen Transit von Daten angebracht, auch wenn diese auf dem Transit durch HW- und SW-Komponenten laufen, die sich im Inland befinden. Erfolgt hingegen ein Verarbeitungsschritt im Inland, der nicht durch fernmeldetechnische oder Steuerungs-Gründe bedingt ist, findet das nationale Gesetz Anwendung, weil das einheimische Rechtsgebiet nicht bloss passiert wird, sondern ein durch einen weiteren Verwendungszweck der Daten bedingter Verarbeitungsvorgang vorgenommen wurde, womit der Transitbegriff nicht mehr zutrifft.

Die mit dem reinen Transit verbundenen Verarbeitungen sollten nicht nur eine Sonderregelung gegenüber den normalen, datenverarbeitenden Vorgängen erfahren, ein nationales Gesetz sollte zugleich die Eingriffe in die Transitwege und Transitdatenflüsse schlechthin untersagen.¹⁰⁸

108 Vorbehältlich systemtechnischer Eingriffe, die bei Fehlern und Mängeln des Netzes oder der Uebermittlung notwendig sein können.

109 Vgl. vorne, S. 293f.

B. Verletzung oder unbefugte Eingriffe in Transitdaten

Das nationale Recht muss geeignete Massnahmen und Sanktionen für den Fall vorsehen, dass während der Transitphase der Daten durch das Inland unbefugterweise Handlungen vorgenommen werden, die den Transit stören oder zu Persönlichkeitsverletzungen führen. Der Eingriff und die Verletzung würden somit nach einheimischem Recht beurteilt, und gemäss dem Territorialitätsprinzip wäre auch die inländische Zuständigkeit gegeben. Für die rechtliche Ausgestaltung sollte berücksichtigt werden, dass mit einem Eingriff u.U. auch das Fernmeldegeheimnis verletzt sein könnte, je nachdem an welcher Stelle der unbefugte Eingriff in ein Datennetz oder eine Fernmeldeverbindung erfolgt ist.

C. Vorbehalt einer abweichenden Regelung durch ein internationales Rechtsregime

Verschiedene national voneinander abweichende Regelungen der Transitfrage können u.U. die Gefahr von Gesetzeskollisionen und -lücken im internationalen Verkehr schaffen.¹⁰⁹ Es ist daher angezeigt, die nationale Norm im Hinblick auf eine internationale Vereinbarung mit abweichendem Inhalt zu relativieren und in einer nationalen Regelung einen entsprechenden Vorbehalt aufzunehmen.

6. "Rechtshilfe" i.S. von Rechtsbeistand

A. Regelung ohne Berücksichtigung einer internationalen Vereinbarung

Da vor allem im internationalen Verkehr das Datensubjekt bei der Ausübung seiner Individualrechte oft überfordert ist, sind Bestimmungen zu erlassen, die dem Betroffenen von behördlicher Seite Rechtshilfe und einen gewissen Beistand gewähren, falls die Wahrnehmung eines Rechtes auf internationaler Ebene zur Frage steht. Die komplexen Verflechtungen der internationalen Datenverarbeitungs- und Datenschutzszene dürfen den Betroffenen nicht zum Verzicht auf die Geltendmachung seiner Rechte und damit zur Duldung einer Verletzung seiner Persönlichkeitsrechte veranlassen.

Die Rechtshilfe bzw. Rechtsbeistand konzentriert sich bei fehlenden internationalen Abkommen allein auf die inländischen Behörden,¹¹⁰ die auf die Zusammenarbeit mit ausländischen Behörden angewiesen sind. Dass eine solche Zusammenarbeit nicht garantiert ist, solange sie weder auf zwischenstaatlichen, noch auf internationalen Abkommen beruht, beschränkt die Effizienz der Behörde und verdeutlicht die Tatsache, dass sie von der Kooperationsbereitschaft ausländischer Stellen abhängig ist. Die Nützlichkeit der Rechtshilfe ist wohl nicht zu bestreiten, aber an ihr Wirkungsvermögen dürfen nicht zu hohe Erwartungen geknüpft werden.

a) Legitimation

Die Legitimation zur Inanspruchnahme der Rechtshilfe muss jedem Rechtssubjekt zustehen, dessen personenbezogene Daten vom Anwendungsbereich des Gesetzes erfasst werden und am grenzüberschreitenden Verkehr teilnehmen.

Somit hätten nach dem Prinzip der Gleichbehandlung des Schutzes personenbezogener Daten sowohl Inländer als auch Ausländer Anspruch auf die Rechtshilfe der nationalen Behörden.

Dabei muss allerdings darauf geachtet werden, dass Ausländer, deren Daten durch den grenzüberschreitenden Fluss ins Inland gelangten, die inländischen Behörden nicht übermäßig beanspruchen, weil sie von der Datenschutzbehörde des Ursprungslandes keine entsprechende Rechtshilfe erhalten. In dieser Beziehung wäre u.U. das Prinzip der Gleichbehandlung zu relativieren und von der Reziprozität, d.h. der Kooperationsbereitschaft der ausländischen Behörde (im Ursprungsland) abhängig zu machen.

b) Gegenstand der Rechtshilfe bzw. des Rechtsbeistandes

Die Rechtshilfe bzw. Rechtsbeistand kann sich dem Datensubjekt aber auch der verantwortlichen Stelle auf verschiedene Arten als nützlich erweisen.

110 I.e. Datenschutzbehörden

aa) Wahrung der Individualrechte

Damit den Individualrechten im internationalen Datenfluss auch Nachdruck verliehen wird, sollte sich m.E. die Rechtshilfe in erster Linie auf deren Geltendmachung und Verwirklichung im Ausland beziehen. Dabei sind aufgrund der verschiedenartigen Ansprüche die Individualrechte entsprechend den Verfahren beispielsweise einteilbar in Individualrechte, welche in streitigen und nichtstreitigen Verfahren geltend gemacht werden.¹¹¹

aaa) Individualrechte in nichtstreitigen Verfahren

Bei Individualrechten,¹¹² die in nichtstreitigen Verfahren geltend gemacht werden können, kann sich die Rechtshilfe z.B. in der Ueberweisung des Begehrens und dessen Anmeldung bei der verantwortlichen Stelle erschöpfen. Rechtshilfe sollte hier in ausgedehnterem Masse gewährt werden, da diese Ansprüche auch die Funktion einer Individualkontrolle haben und zur Qualität der Daten beitragen. Eine höhere Datenqualität vermindert aber die Gefahr der Persönlichkeitsverletzungen. Auch die Uebersetzung von erteilten Auskünften wäre zu erwägen und in der Rechtshilfe einzuschliessen.

bbb) Individualrechte in streitigen Verfahren

Die Fälle,¹¹³ in denen die Ansprüche aus dem Datenschutz in Form eines parteiförmigen Rechtsstreites geltend gemacht werden, erheischen eine andere Form der Rechtshilfe, als jene für die Durchsetzung von Ansprüchen in der freiwilligen Gerichtsbarkeit. Hier könnte die Rechtshilfe z.B. in einer Rechtsberatung vor der Klageerhebung bestehen; u.U. sind auch Ueberprüfungen und Expertisen durch entsprechende Spezialisten denkbar, die dem Betroffenen eine Orientierung

111 Vgl. auch GULDENER; S. 41ff.

112 Z.B. Auskunftsrecht, Einsichtsrecht, Besichtigungsrecht etc.

113 Z.B. Unterlassungsklage, Schadenersatzklage, Genugtuungsklage etc.

ermöglichen, wie seine Erfolgsaussichten im Ausland resp. bei einem international mit mehreren Staaten verknüpften Tatbestand zu beurteilen sind. Ferner könnte sich die Rechtshilfe auch auf die Beurteilung Zuständigkeitsfragen sowie die Art und Form der Klageerhebung beziehen.

bb) Kostenlast

Charakteristisch für internationale Tatbestände sind die erhöhten Kosten, die für Uebersetzungen, Gutachten, Rechtsauskunft und -beratung, Verifikationen, Experten und Spezialisten etc. aufgewendet werden müssen. Es wäre aber untragbar, wenn die Kostenlast zur Ursache eines Verzichts auf die Wahrnehmung der Individualrechte auf internationalem Gebiet führen würde. Es muss deshalb ein Weg gefunden werden, jedem Datensubjekt die Ausübung der Individualkontrolle zu ermöglichen und deren Durchsetzung zu unterstützen: In diesem Sinne sollte ein sogenanntes "soziales Datenschutzrecht" angestrebt werden.

Es sind mehrere Möglichkeiten denkbar, die dem Betroffenen Hilfe bei der Tragung der Kostenlast gewähren:

- So könnten z.B. Rechtsauskunft und Rechtsberatung durch die Datenschutzbehörde gegen eine bestimmte feste Gebühr ¹¹⁴ erteilt werden. Diese Stelle scheint für nationale wie internationale Rechtsfälle am kompetentesten zu sein, da ein solches Organ i.d.R. viel Erfahrung aus dem Umgang mit ausländischen Stellen bzw. Datenschutzgesetzen besitzt und deshalb den wirksamsten Rechtsdienst zur Verfügung stellen könnte.
- Es ist denkbar, dass von der Datenschutzbehörde Uebersetzungskosten, die bei der Ausübung von Individualrechten in nicht strei-

114 Eine Gebühr ist notwendig, damit diese Stelle nicht mit einer Fülle von Anträgen und Begehren überschüttet wird. Es muss dabei eine Differenzierung nach der wirtschaftlichen Leistungsfähigkeit des Datensubjektes vorgenommen werden. Eine entsprechende Regelung müsste verhindern, dass kapitalkräftige juristische Personen von der behördlichen Rechtshilfe, die prinzipiell für die natürlichen Personen konzipiert ist, profitieren.

tigen Verfahren anfallen, gegen Gebühr veranlasst werden; (es wird sich hier z.B. um die Uebersetzung von Auskunftsbegehren und der erteilten Auskünfte handeln).

- Zugunsten von Datensubjekten, welche die hohen Kosten aus der Erstellung von Gutachten oder dem Beizug von Spezialisten nicht bestreiten können, müsste aufgrund von Art. 4 BV - analog dem Institut des Armenrechts¹¹⁵ bzw. der unentgeltlichen Prozessführung¹¹⁶ - die Uebernahme dieser Kosten durch den Staat in Betracht gezogen werden. Voraussetzung zur Ueberwälzung der Kostenlast auf den Staat wären z.B. das Fehlen der nötigen Geldmittel und die Chancen auf einen günstigen Prozessausgang; (letzteres Erfordernis ist bei Gutachten allerdings relativiert zu betrachten, da die Chancen des Prozessausganges oft erst nach Vollzug einer Expertise zu beurteilen sind).
- U.U. ist für ausländische Rechenzentren, welche verarbeitende Tätigkeiten im Inland ausüben wollen, eine Norm denkbar, die die Hinterlegung einer Kautions vorschreibt.^{117 118}

cc) Unterstützung einer verantwortlichen Stelle

Die hier vorgeschlagene Art der Rechtshilfe wäre nicht allein auf die Unterstützung der von der Datenverarbeitung betroffenen Personen ausgelegt, sondern wäre m.E. auch für die mit dem grenzüberschreitenden Datenverkehr tätigen verantwortlichen Stellen erforderlich und nützlich.

Es ist vor allem eine beratende Art der Rechtshilfe gegenüber verantwortlichen Stellen denkbar, die sich auf die Erteilung von Auskünften über verarbeitungs- und schutzspezifische Fragen beim grenzüberschreitenden Datentransport konzentriert; sie könnte aber auch als zuständige Vermittlungsstelle für die Interessen verantwortlicher Stellen im Inland fungieren, falls die Vollstreckung von ausländi-

115 GULDENER, S. 410f.

116 WALDER, S. 383f.

117 Vgl. spanischer Entwurf zu BG über Schutz personenbezogener Daten vom 17.12.1975: Art. 29 Abs. 2.

118 SIMITIS, Festschrift, S. 362f.

schen Entscheiden den Geschäftszweck des inländischen Datenverarbeiters gefährden und deshalb ein Vollzug aufgeschoben werden sollte. Für solche Leistungen an verarbeitende Stellen wäre m.E. ein angemessenes Entgelt (Gebühr) vorzusehen.

c) Vollstreckung ausländischer Urteile und Entscheidungen

Aus dem Prinzip der Gleichbehandlung in- und ausländischer Daten-subjekte sollte auch ein Rechtshilfemittel zur Verfügung gestellt werden, das die Vollstreckung ausländischer Urteile und Entscheidungen im Inland gewährleistet. Die spezifische Ausgestaltung einer entsprechenden Norm wird sich zweckmässigerweise am Vorbild bereits bestehender Abkommen und der Praxis orientieren müssen. Es ist allerdings nicht weiter hervorzuheben, dass die Anrufung des "ordre public" verhindern kann, dass Urteile, die der inländischen Rechtsordnung widersprechen, nicht vollstreckt werden können.

B. Regelung im Hinblick auf eine internationale Vereinbarung

Da Rechtshilfe und internationale Zusammenarbeit im Bereich von völkerrechtlichen Vereinbarungen eine bedeutende Rolle spielen,¹¹⁹ müsste die vom nationalen Gesetz vorgesehene Rechtshilfe einem Rechtshilfesystem im Rahmen eines internationalen Uebereinkommens im Interesse einer einheitlichen Normierung und Rechtsdurchsetzung den Vorrang geben. Es ist somit unerlässlich, nationale Normen über Rechtshilfe bzw. Rechtsbeistand durch den Vorbehalt einer abweichenden internationalen Vereinbarung zu relativieren.

C. Massnahmen zum Schutz der Rechtshilfe

Das nationale Recht hätte Massnahmen zu erlassen, die sicherstellen, dass die Rechtshilfe nicht missbräuchlich angerufen und ausgenutzt werden kann, sei es von Behörden (national wie international), sei es von privaten Stellen. Es wäre unerträglich, wenn die durch Rechtshilfe erlangten Informationen durch zweckentfremdete Verwendung zu neuen Persönlichkeitsverletzungen führen würden.

119 vgl. KE und RL, vorne, S. 261ff. und 279ff.

7. Bestimmung über die Datenqualität im internationalen Bereich

Im internationalen Kontext kann die Nachführung, Ergänzung, Löschung, Korrektur von importierten bzw. übermittelten Daten wegen der komplizierten Rechtsverhältnisse und des beschränkten Anwendungsbereiches nur mit einer internationalen Vereinbarung abschliessend geregelt werden, doch wäre eine entsprechende Norm auf nationaler Ebene ein Beitrag zur Erhöhung der Datenqualität der dem grenzüberschreitenden Datenverkehr unterworfenen personenbezogenen Informationen.

Die Norm muss im privaten Bereich berücksichtigen, dass die Forderung nach Korrektheit und Aktualität nicht so weit gehen darf, dass sie eine kontraproduktive Wirkung auf den Schutz der Privatsphäre hat.¹²⁰

Eine entsprechende Bestimmung ist in der Form denkbar, dass jede datenverarbeitende Stelle, die Daten aus dem Ausland empfängt,¹²¹ verpflichtet wäre, von der exportierenden Stelle mitgeteilte Nachführungen, Ergänzungen, Korrekturen an den Daten zu vollziehen und diese gegebenenfalls nach den Weisungen des ausländischen Bearbeiters der einer ausländischen Behörde sogar zu löschen. Umgekehrt müsste jeder exportierenden Stelle die Pflicht auferlegt werden, die durch die Individualkontrolle, aber auch im Rahmen der Fremd- und Selbstkontrolle bewirkten Aenderungen, Korrekturen, Sperrungen, Löschungen an diejenigen Stellen weiterzuleiten, die Empfänger der Daten waren. Damit diese Korrektur- und Weiterleitungspflicht nicht ein unüberschaubares Ausmass annimmt, ist es u.U. sinnvoll, sie nur auf Daten anzuwenden, die innerhalb eines gewissen Zeitraumes übermittelt wurden (z.B. während der letzten zwei Jahre).

¹²⁰ Vgl. vorne, S. 252.

¹²¹ Hierzu gehört auch der Benutzer einer ausländischen Datenbank, der lediglich Zugriff auf die Daten, aber keine Verfügungsgewalt hat: Er kann vom Betroffenen gemeldete Fehler weder korrigieren noch Ergänzungen bzw. Löschungen vollziehen. Diesfalls sollte eine Weiterleitungspflicht der Aenderungen, Ergänzungen an die verantwortliche Stelle der Datensammlung statuiert werden, damit die Unrichtigkeiten und Mängel dem Datenbankführer zu Kenntnis kommen.

8. Spezielle Datensicherungsvokehrungen

Datenschutznormen allein genügen nicht zum Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr, es sind zusätzlich spezielle Datensicherungs Vorschriften auszuarbeiten.

M.E. hat die Datensicherung einen bedeutenden, nicht zu unterschätzenden Stellenwert bei der Vermeidung von Persönlichkeitsverletzungen anlässlich einer Uebermittlung von personenbezogenen Daten ins Ausland.¹²² Die Datensicherungsaspekte müssen deshalb in einer Regelung der transnationalen Datenflüsse auch zum Ausdruck kommen. Dabei ist wichtig, dass die Vorkehrungen der Datensicherung sowohl in der Uebermittlungsphase, die über andere Territorien oder via Satellit ins Bestimmungsland führen kann, als auch in der Verarbeitungsphase im Ausland für die Sicherheit der Daten sorgen.

Auf die Sicherungsmassnahmen während der Uebermittlungsphase kann die nationale Gesetzgebung direkt Einfluss nehmen, indem sie bestimmte Datensicherungskomponenten für den Export bzw. Import von Daten vorschreibt. Eine solche Vorschrift hat aber auch gewisse indirekte Auswirkungen beim Empfänger bzw. Absender im Ausland, weil die entsprechenden Sicherungseinrichtungen bei Uebermittlungen sowohl auf Sender- wie Empfängerseite vorhanden sein müssen (z.B. Verschlüsselungsgeräte, Verschlüsselungsprogramme).

Auf die Datensicherungsvokehrungen während der Verarbeitung im Ausland hat das nationale Recht keinen unmittelbaren Einfluss, da sich die verarbeitende Stelle im Ausland ausserhalb des gesetzlichen Geltungsbereiches befindet; das nationale Gesetz kann jedoch in einem gewissen Masse Einfluss auf die verantwortliche Stelle im Ausland nehmen, indem es der exportierenden Stelle eine bestimmte Genehmigungsart (z.B. nur Einzelgenehmigung oder Mustergenehmigung oder sogar Konzession) für die Ausfuhr von Daten erteilt.⁵⁴ Da meistens

122 G1. M. FREESE, Data Flow, S. 52 und 69f.

die empfangende und verarbeitende Stelle im Ausland am transnationalen Verkehr interessiert sind, kann direkt gefordert werden, dass auch auf der Verarbeiterseite gewisse (Mindest-) Normen erfüllt sind - es ist aber auch denkbar, dass mit einzelnen Genehmigungstypen Auflagen für die exportierende Stelle und den verarbeitenden Empfänger im Ausland gemacht werden.

Die durch den Erlass nationaler Datensicherungsvorschriften bewirkte Ausdehnung des Geltungsbereiches wird i.d.R. nicht zu einer Gesetzeskollision mit den Vorschriften des Empfangsstaates führen, da die Sicherungsvorkehrungen weltweit auf den gleichen Prinzipien beruhen, datenverarbeitungsspezifisch geprägt sind und deshalb nicht von einem Rechtssystem bzw. einem nationalen Kontext, Kulturkreis und Entwicklungsstand abhängen.

Im Hinblick auf internationale Vereinbarungen sollte das nationale Gesetz einen Vorbehalt für neue internationale Standards oder spezifische Abkommen (z.B. Satellitenverkehr) aufnehmen.

Die detaillierte Ausgestaltung erhöhter nationaler Datensicherungsanforderungen beim grenzüberschreitenden Datenverkehr muss den Informatikern überlassen bleiben.

III. Massnahmen und Sanktionen bei Verletzungen materieller und formeller Normen zum grenzüberschreitenden Datenverkehr

1. Zuordnung der Verantwortlichkeit

Die Verantwortlichkeit für Missbräuche und Rechtsverletzungen im internationalen Datenverkehr sollte mit derjenigen des nationalen Datenverkehrs identisch sein. Der Gesetzgeber hat somit jene Stelle zu bezeichnen, die für Verfehlungen und Rechtsverletzungen zivilrechtlich, administrativ als auch strafrechtlich verantwortlich gemacht

123 So können z.B. Datensicherungsvorkehrungen und gesellschaftsinterne Datenschutzrichtlinien, wie ein Verhaltenskodex, beim Empfänger in Ländern ohne Datenschutzrecht ausschlaggebend für die Erteilung einer Ausfuhrgenehmigung sein (z.B. für eine Konzession bei multinationalen Gesellschaften).

werden kann. Die Festlegung dieser verantwortlichen Stelle, d.h. jene juristische oder natürliche Person (ev. sogar Personengruppen, Vereinigungen), die Datenbearbeitung betreibt und Datensammlungen mit personenbezogenen Informationen unterhält, erfolgt nach dem Kriterium der verarbeitungsspezifischen Entscheidungsbefugnis.¹²⁴ Verantwortlich ist also diejenige Stelle, die Ziel, Zweck, Art und Weise der Datenverarbeitung bestimmt und über Auswahl, Gebrauch, Verarbeitung und Nutzung der Datei entscheidet. Mit der Bezeichnung dieser Stelle ist die Passivlegitimation für Ansprüche, Sanktionen und Massnahmen gegeben, falls eine verantwortliche Stelle Daten ein- oder ausführt und dabei eine Rechtsverletzung begangen hat.

2. Zweck und Inhalt

Mit einem Konzept von Sanktionen und Massnahmen, die diejenigen des nationalen Datenverkehrs ergänzen, muss der Beachtung der gesetzlichen Normen zum grenzüberschreitenden Datenverkehr gegenüber den verantwortlichen Stellen Nachdruck verliehen werden, um eine präventive Wirkung zu erreichen, die eine Verletzung der Persönlichkeitsrechte durch die Missachtung dieser Normen vermeiden hilft.

Die materielle Ausgestaltung dieser Massnahmen und Sanktionen hat die "Rentabilität" einer Umgehung des Gesetzes nach Möglichkeit auszuschliessen. Ausserdem muss dem Präventivgedanken ein bedeutender Stellenwert eingeräumt werden: Er könnte einerseits darin zum Ausdruck kommen, dass die zivilrechtlichen Sanktionen (Genugtuung, Schadenersatz usw.) aufeinander abgestimmt werden, sich gegenseitig ergänzen und u.U. sogar eine Interdependenz bzw. Kumulation bei ihrer Anwendung zugelassen wird; andererseits wäre ein Abschreckungseffekt auch durch entsprechende Strafbestimmungen, vor allem hohe Geldbusen,¹²⁵ durch einschneidende administrative Massnahmen (z.B. Ver-

124 Vgl. andere Gesetze (AU) sowie KE und RL.

125 Strafnormen sind dabei für die schweren Verletzungsformen angebracht z.B. bei Absicht, (Eventual-) Vorsatz sowie u.U. grober Fahrlässigkeit.

bot des grenzüberschreitenden Datenverkehrs für einen bestimmten Zeitraum, Zwangslöschung von Daten usf.) sowie durch strengere zivilrechtliche Sanktionen (z.B. durch erleichterte Voraussetzungen für den Anspruch auf Schadenersatz und evtl. [höhere] Genugtuung) zu erreichen.

Ein erhöhtes Haftungsrisiko, gekoppelt mit einschneidenden administrativen Massnahmen und einer angemessenen Strafdrohung, wäre m.E. geeignet, die verantwortlichen Stellen von der Vornahme eines rechtswidrigen Exportes bzw. Importes mit einer daraus resultierenden Persönlichkeitsverletzung wirksam abzuschrecken.

Sanktionen und Massnahmen müssen entsprechend dem Grad des Verschuldens und der Intensität der Persönlichkeitsverletzung abgestuft angeordnet werden, doch sollte auch für die leichtesten Verschuldensformen noch eine Sanktion vorgesehen sein, um die verantwortlichen Stellen zu einer erhöhten Aufmerksamkeit bei grenzüberschreitenden Datenverschiebungen zu veranlassen. Sanktionen und Massnahmen können aber nur die verantwortlichen Stellen des Inlandes treffen, welche unter Missachtung einer Vorschrift über den grenzüberschreitenden Datenverkehr des inländischen Rechts zur Verletzung der Persönlichkeit eines Rechtssubjekts beigetragen haben, auch wenn die Verletzung erst im Ausland erfolgt, die Missachtung nationalen Rechts aber eine Ursache oder Teilursache der Verletzung des Persönlichkeitsrechtes darstellt. Ist hingegen der Export und Import gemäss den Vorschriften des nationalen Gesetzes vollzogen worden und der Verletzungstatbestand durch die Verarbeitung nach Massgabe ausländischer Normen im Ausland begründet, wären die einheimischen Sanktionen und Massnahmen nicht anwendbar.

Eine gleichzeitig präventive und repressive Wirkung hätten flankierende Normen: Z.B. die Vorschrift, dass die aus der Geltendmachung von Ansprüchen im Rahmen der Rechtshilfe entstandenen Kosten (Expertise, Übersetzungskosten etc.) der fehlerhaften verantwortlichen Stelle überbunden werden.

IV. Verhältnis des grenzüberschreitenden Datenverkehrs zum
Art. 273 StGB

Art. 273 StGB hat in der Rechtsprechung eine Ausweitung des Tatbestandes ¹²⁶ erfahren, die im Zusammenhang mit einer nationalen wie internationalen Regelung des grenzüberschreitenden Datenverkehrs überprüft werden muss.

Zentraler Begriff ist das "Fabrikations- und Geschäftsgeheimnis", das gemäss Rechtsprechung ¹²⁷ "alle Tatsachen des wirtschaftlichen Lebens, an deren Geheimhaltung ein schutzwürdiges Interesse besteht" umfasst; er ist gemäss BGr. ¹²⁸ weit auszulegen. Dieses Geheimhaltungsinteresse privater Personen ist durch das Interesse des Staates überlagert, die unter seiner Gebiets- und Rechtssicherheit befindlichen natürlichen und juristischen Personen gegen Auskundschaftung und Preisgabe von wirtschaftlichen Informationen zu schützen. Dieser Anspruch auf Schutz gesamtschweizerischer Interessen geht soweit, dass keine direkte Schädigung oder Gefährdung der staatlichen resp. privaten materiellen Interessen notwendig ist, sondern bereits jede nachrichtendienstliche Tätigkeit im Bereich der Wirtschaft als "mittelbare Verletzung oder Gefährdung der staatlichen Interessen" ¹²⁹ gilt und den Tatbestand von Art. 273 StGB als abstraktes Gefährdungsdelikt erfüllt.

Weiteres Erfordernis ist, dass der wirtschaftliche Nachrichtendienst zugunsten eines fremden staatlichen oder privaten Unternehmens, einer ausländischen amtlichen Stelle oder Organisation durch ein Auskundschaften oder blosses Zugänglichmachen erfolgt. Die mit blossem Zugänglichmachen umschriebene Tathandlung erlaubt eine äusserst extensive Auslegung des Tatbestandes.

126 STRATENWERTH, Bd. II, S. 252.

127 BGE 98 IV 210.

128 BGE 101 IV 199, Erw. 4a.

129 BGE 98 IV 211 / BGE 101 IV 313.

Der Austausch wirtschaftlicher Informationen und Daten über die nationalen Grenzen hinweg, ist angesichts der heutigen internationalen Wirtschaftsbeziehungen nicht nur ein notwendiger, sondern zugleich ein im Hinblick auf die nationale Volkswirtschaft legitimer Vorgang.¹³⁰

Die durch den Art. 273 StGB verursachten Unklarheiten infolge extensiver Auslegung und Anwendungspraktiken schildert STRATEN-WERTH¹³¹ zutreffend: "Jede Weitergabe wirtschaftlicher Informationen über die Landesgrenzen hinweg kann auf diese Weise zum verbotenen Nachrichtendienst werden. Das Ergebnis ist auch hier ein Höchstmass an Rechtsunsicherheit. ... Was verboten und was erlaubt ist, kann unter diesen Umständen niemand wissen."

Solche Rechtsunsicherheit erzeugenden Normen sind im Kontext eines freien Informationsaustausches absolut unerträglich.

Die Vorschrift kann mit ihrer extensiven Auslegung des Begriffes des Geschäfts-/Fabrikationsgeheimnisses erhebliche negative Einwirkungen auf eine nationale Regelung des grenzüberschreitenden Datenverkehrs haben und bedarf deshalb einer Analyse, Ueberprüfung und Beschränkung ihres Anwendungsbereiches, da sie in der gegenwärtigen Form nicht mehr mit den modernen Kommunikationsmethoden des privaten und öffentlichen Bereiches vereinbar ist. Es entspricht sicher nicht der ratio legis des Gesetzgebers, den durch internationale Verflechtungen bedingten grenzüberschreitenden Verkehr mit Daten aus dem Wirtschaftsleben als Preisgabe von Geschäftsgeheimnissen, d.h. zum Delikt gegen den Staat, zu deklarieren und zu unterbinden. Der Zweck der Bestimmung bleibt auch bei einer restriktiven Anwendung bestehen, aber die extensive Auslegung durch die Rechtsprechung¹³² muss an die heutigen tatsächlichen Verhältnisse angepasst und die bestehende Rechtsunsicherheit beseitigt werden.

130 Vgl. vorne, Notwendigkeit des grenzüberschreitenden Datenverkehrs, S. 1ff.; gl. M. STRATENWERTH, Bd. II., S. 255.

131 Bd. II, S. 253.

132 Höchst protektionistisch erscheint die Tatsache, dass auch ein vertragswidriges oder ein im Ausland als illegal geltendes Interesse als schützenswert zugunsten der schweizerischen Volkswirtschaft betrachtet wird: BGE 101 IV 312ff.

Der Art. 273 StGB darf m.E. nicht dazu missbraucht werden, mit Hilfe einer schrankenlosen Auslegung einheimische partikuläre Wirtschaftsinteressen gegenüber möglichen negativen Auswirkungen¹³³ des grenzüberschreitenden Datenverkehrs, die innerhalb eines freien Wettbewerbs und einer liberalen Wirtschaftsordnung durchaus auftreten können, zu protegieren. Die Wettbewerbsneutralität des Datenschutzes muss sowohl auf nationaler Ebene wie im internationalen Rahmen aufrechterhalten werden und hat auf die Anwendung des Art. 273 StGB insofern Einfluss, als der reguläre Export einheimischer personen- und sachbezogener Daten nicht als Erfüllung des Tatbestandes von Art. 273 StGB qualifiziert werden darf. Eine derartige, einseitige Unterbindung des Informationsverkehrs widerspricht nicht nur dem Prinzip des freien Datenflusses, wie er in internationalen Vereinbarungen (KE, RL) vorgesehen ist, er steht auch nicht im Einklang mit den tatsächlichen Wirtschaftsinteressen unseres Landes, die heute andere Informationsmethoden voraussetzen als zur Zeit der Schaffung der Strafnorm des Art. 273 StGB.¹³⁴

V. Nationale Kollisionsnormen¹³⁵

Wie vorne¹³⁶ ausgeführt, würde die Ausarbeitung konkreter Lösungsmodelle von nationalen Kollisionsnormen den Rahmen dieser Arbeit sprengen. Ich beschränke mich deshalb auf einige grundlegende Überlegungen, die bei der Ausarbeitung eines Datenschutzgesetzes im allgemeinen und bei der Entwicklung nationalen Kollisionsnormen zum Datenschutz im besonderen aufgestellt werden können.

Die Notwendigkeit der Aufnahme von Kollisionsnormen in ein schweizerisches Datenschutzrecht folgt aus der Zielfunktion des Datenschutzes, auf Erlass geeigneter Vorschriften für einen effektiven Schutz der Persönlichkeitssphäre. Dieser Schutz verlangt nicht nur

133 Z.B. Verlust an Arbeitsplätzen durch DV im Ausland.

134 Art. 273 war ursprünglich nicht im StGB, sondern in dem sog. "Spitzelgesetz" aus der Mitte der 30er Jahre."

135 Vgl. vorne, S. 295ff.

136 S. 299.

die Gewährleistung des Persönlichkeitschutzes im landesinternen Bereich, sondern auch die Aufstellung von Vorschriften des materiellen IPR zum Schutz personenbezogener Daten im grenzüberschreitenden Datenverkehr, ebenso wie den Erlass von Bestimmungen zur Lösung von Gesetzeskonflikten.

Im Hinblick auf die Ursachen von Gesetzeskonflikten sollte in einem nationalen Datenschutzgesetz bezüglich der Normen, die den grenzüberschreitenden Datenverkehr regeln, eine Ausdehnung des gesetzlichen Anwendungsbereiches auf ausländische Verarbeitungsvorgänge und verantwortliche Stellen wenn möglich vermieden werden.¹³⁷ Der Gesetzgeber muss darauf achten, dass die Anwendbarkeit der Bestimmungen auf die innerhalb seines Territoriums erfolgenden Verarbeitungs- und Benutzungshandlungen beschränkt bleibt.

Für die Schaffung und materielle Ausgestaltung einer Kollisionsnorm besitzt der Gesetzgeber aber nicht beliebige Variationsmöglichkeiten; er ist vielmehr aufgrund der Rechtsordnung und der nationalen Datenschutzgesetzgebung an bestimmte Schranken gebunden, d.h. die nationale Gesetzgebung hat einen entscheidenden Einfluss auf die Ausgestaltung einer Kollisionsnorm. Dieser Einfluss ist daran erkennbar, dass der materielle Inhalt eines Datenschutzgesetzes nicht losgelöst von den Anknüpfungsregeln bestimmt werden kann und eine Anknüpfung immer im Kontext des nationalen Gesetzes eingebettet sein muss.¹³⁸

137 Ausnahmsweise sind Vorschriften für Datensicherungsmassnahmen denkbar (vgl. vorne, Nr. III, 8, S. 379ff.).

138 Erfolgt z.B. die Anknüpfung an der verantwortlichen Stelle, bedeutet dies, dass das nationale Gesetz entsprechend aufgebaut sein muss und eine Definition der verantwortlichen Stelle gibt sowie deren Identifizierung ermöglicht, z.B. durch Registrierung von Datenbanken, und ferner verhindert, dass verantwortliche Stellen bzw. Datensammlungen ohne weiteres verschoben werden können. Es sollte diesfalls eine Bestimmung erlassen, welche die bloss deklaratorische Bezeichnungen eines Sitzes verunmöglicht und dafür sorgt, dass der Sitz einer verantwortlichen Stelle, deren Host-Computer (Zentralrechner, Leitsystem) eines Datenverbundsystems im Inland liegt, nicht durch eine deklaratorische Sitzänderung ins Ausland verlegt werden kann, sondern ebenfalls im Inland begründet wird.

M.E. hat sich die Wahl des Anknüpfungspunktes am Schutzzweck des Datenschutzgesetzes zu orientieren und dem Datensubjekt im internationalen Bereich eine günstige Ausgangslage für die Wahrnehmung seiner Rechte zu schaffen. Der Anknüpfungspunkt darf aber nicht alleine zum Vorteil des Datensubjektes ausgestaltet sein, sondern muss auch die Interessen der datenverarbeitenden Stellen berücksichtigen und einen Interessensausgleich vornehmen: So ist z.B. eine Berücksichtigung der Interessen durch eine unterschiedliche Anknüpfung nach der Art der Ausübung von Individualrechten denkbar:

- Die Individualrechte, die in nichtstreitigen Verfahren¹³⁹ geltend gemacht werden, wie z.B. Auskunft, Einsicht, Berichtigung usw., sollten eine möglichst nahe Anknüpfung beim Datensubjekt erfahren, d.h. die Wahl des Anknüpfungspunktes muss auf das Recht fallen, das dem Datensubjekt die Ausübung seiner Ansprüche möglichst leicht macht, weil es ihm vertraut ist. Es liegt sicher auch im Interesse der verantwortlichen Stelle, wenn die Ausübung dieser Ansprüche für das Datensubjekt durch die gewählte Anknüpfungsform "attraktiv" erscheint, da diese Individualrechte letztlich dazu dienen, die Datenqualität zu erhöhen. An der Richtigkeit der Daten ist i.d.R. nicht allein der Betroffene interessiert, sondern auch der Verarbeiter und Benutzer der personenbezogenen Informationen, da die Qualität der Daten zu Vermeidung von Persönlichkeitsverletzungen beiträgt.

Eine solche auf das Datensubjekt ausgerichtete Anknüpfung bedeutet für den Gesetzgeber die Schaffung von Normen, welche die verantwortliche Stelle beim grenzüberschreitenden Datenverkehrs verpflichten, die in nichtstreitigen Verfahren geltend gemachten und dem Betroffenen zustehenden Ansprüche¹⁴⁰ an ausländische Empfänger weiterzuleiten.¹⁴¹

139 Vgl. vorne, III., 6., A., b), aa) aaa), S. 365.

140 Z.B. Korrektur.

141 Vgl. vorne, III. Nr. 7, S. 378.

- Die andere Gruppe der Individualrechte¹⁴² sowie die übrigen, aus einem Datenschutzgesetz folgenden Ansprüche und Rechtsfolgen,¹⁴³ die in streitigen Verfahren¹⁴⁴ ausgetragen werden und ein Urteil oder eine Verfügung einer richterlichen oder administrativen Behörde voraussetzen, damit der Entscheid vollstreckt werden kann, sind nach dem hier vorgeschlagenen Konzept näher bei der verantwortlichen Stelle anzuknüpfen. Die aus der Geltendmachung dieser Rechte resultierenden Verantwortlichkeiten und die Notwendigkeit der Vollstreckung der Urteile rechtfertigen eine Anknüpfung in der Nähe der verantwortlichen Stelle, da sie sich dem Entscheid unterziehen muss.

Die Rechtswahl in der Nähe der verantwortlichen Stelle ist aber auch für den Betroffenen vorteilhaft, da einer Vollstreckung des Entscheides keine rechtlichen Hindernisse entgegenstehen. Die ungünstigere Lage des Datensubjektes bei der Geltendmachung könnte z.B. durch einen entsprechenden Ausbau der Rechtshilfe bei der Wahrnehmung dieser Rechte nach ausländischem Verfahrensrecht ausgeglichen werden.

Dieser Vorschlag einer Aufteilung der möglichen Anknüpfungspunkte im privaten Sektor erfolgt aus rein pragmatischen Gründen und lässt sich hinsichtlich der Ansiedlung in der Nähe des Betroffenen für Ansprüche in nichtstreitigen Verfahren durch die Häufigkeit ihrer Geltendmachung begründen, während die Anknüpfung am Sitz der verantwortlichen Stelle in den streitigen Verfahren sich durch deren geringere Häufigkeit nur durch eine verstärkte Rechtshilfe und Rechtsbeistand zugunsten des Betroffenen rechtfertigen liesse.

Im Hinblick auf ein internationales Rechtsregime muss aber in der Regelung des grenzüberschreitenden Datenverkehrs auch bei den Kollisionsnormen der Vorbehalt abweichender internationaler Bestimmungen zur Lösung von Gesetzeskonflikten zwischen Mitgliedstaaten

142 Wie z.B. Unterlassungs-, Schadenersatz und Genugtuungsanspruch.

143 Wie z.B. Vollstreckungsanspruch, strafrechtliche Sanktionen.

144 Vgl. vorne, III, 6., A., b), aa), bbb), S. 365.

eingedrängt werden. Bei der Ausarbeitung nationaler Kollisionsnormen empfiehlt es sich deshalb, die Arbeiten internationaler Gremien zu diesem Spezialbereich zu konsultieren und ihre Erkenntnisse zu berücksichtigen, so dass keine erheblichen Abweichungen zwischen den nationalen Kollisionsnormen, die im Verkehr mit Nicht-Mitgliedstaaten einer Konvention zur Anwendung kommen und dem Kollisionsrecht für die Konventionsstaaten entsteht und letztlich dem Datensubjekt eine Orientierung über das anwendbare Recht auch im internationalen Bereich leicht fällt.

§ 14 LOESUNGSVORSCHLÄGE FÜR DEN INTERNATIONALEN BEREICH

I. Lösungsmöglichkeiten zum Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr

Die Probleme bei einer Lösung des grenzüberschreitenden Datenverkehrs werden hauptsächlich von den Interessengegensätzen¹ nach einem möglichst wirksamen Schutz der Persönlichkeit im grenzüberschreitenden Verkehr und dem Postulat nach einem freien nationalen und internationalen Datenfluss ohne protektionistische Schranken oder Hindernisse dominiert. Zusätzlich erweisen sich nationale Interessen hinsichtlich Souveränität, nationaler Sicherheit, wirtschaftlicher und technologischer Entwicklung sowie politische Aspekte als beeinflussende Faktoren für eine Lösung auf internationaler Ebene.

Eine Lösung dieser Interessen und Bestrebungen kann nun auf bilateraler oder supranationaler Ebene in verschiedenen Varianten² verwirklicht werden:

1. Harmonisierung nationaler Gesetze

Diese Variante hat den Nachteil, dass sie nur zwischen Staaten mit gleichen Rechtssystemen und vergleichbarer sozialer Struktur zu verwirklichen ist, so dass sie hauptsächlich auf den zwischen- oder nachbarstaatlichen Bereich und eine Regelung durch bilaterale oder multilaterale Abkommen beschränkt bleibt. Denkbar ist eine solche Lösung z.B. innerhalb von Gemeinschaften wie EG oder den skandinavischen Staaten (Nordischer Rat). Wo die Harmonisierung von Rechtssystemen ihrer Verschiedenheit wegen auf Schwierigkeiten stößt, ist die Vereinbarung der Einhaltung von Gegenrecht (formelle und materielle Reziprozität) in Form bilateraler Verträge denkbar.

1 Vgl. vorne, S. 23ff.

2 CAROLL, S. 206.

Falls solche zwischenstaatliche oder internationale Vereinbarungen fehlen; kann lediglich postuliert werden, dass die nationalen Gesetzgeber ihr Recht möglichst weitgehend dem gemeinsamen Nenner aller Datenschutzgesetze anpassen.³

Der Nachteil zwischenstaatlicher Lösungen liegt in der zunehmenden Unübersichtlichkeit der auf den internationalen Datenverkehr anwendbaren Bestimmungen, was sich in hohen Datenverarbeitungskosten⁴ bei multinational arbeitenden Gesellschaften und Firmen auswirkt, die einen wesentlichen Träger des heutigen internationalen Handels darstellen. Ueberdies befürchten PANTAGES und PIPE⁵ die Bildung von Datenkartellen, die sich aus Harmonisierung oder zwischenstaatlichen Verträgen bei gemeinsamen wirtschaftlichen Interessenbündnissen (wie z.B. EG) ergeben könnten.

2. Vereinbarung minimaler Grundprinzipien

Die Verwendung von Grundprinzipien zum Datenschutz, z.B. nach dem Vorbild der internationalen Erklärung der Menschenrechte durch die Vereinten Nationen, ist eine denkbare Lösungsvariante. Solche Grundprinzipien könnten die Staaten verpflichten, eine minimale Zahl von Grundregeln in ihr nationales Datenschutzrecht aufzunehmen. Angesichts der Vielschichtigkeit der Probleme und den damit verbundenen Gefahren für Individuen, Staat und Wirtschaft, sollte jedoch eine noch grössere Kohärenz zwischen den einzelnen Staaten angestrebt werden, da Grundprinzipien den Problembereich nur an der Oberfläche zu erfassen vermögen.

Als Zwischenstufe, im Hinblick auf ein internationales Abkommen, ist eine Vereinbarung minimaler Grundprinzipien denkbar; eine befriedigende Lösung ist aber von einer solchen Einigung auf den kleinsten gemeinsamen Nenner nicht zu erwarten.

3 BEDNAR/WEISSENBOECK, S. 204.

4 Eine Kostensteigerung kann soweit führen, dass internationale Datenverarbeitungsanwendungen u.U. ökonomisch nicht mehr zu rechtfertigen sind (vgl. EGER, Online, S. 36).

5 PANTAGES/PIPE, S. 115.

3. Internationales Abkommen zur Regelung des grenzüberschreitenden Datenverkehrs⁶

Die beste Lösung, die auf internationaler Ebene einen freien Datenfluss ohne protektionistische Informationsschranken unter einem wirksamen Schutz der Persönlichkeit bietet, ist der Abschluss eines internationalen Abkommens, z.B. in Form einer internationalen Konvention,⁷ das zwischen den Signatarstaaten einen freien Informationsfluss^{8 9} statuiert. Ein internationales Abkommen vermag die von andern völkerrechtlichen Verträgen¹⁰ ausgehenden Einwirkungen adäquat aufzufangen und in entsprechender Weise zu regeln. Trotz der in der Literatur vorhandenen verschiedenen Ansichten über den Rang eines internationalen Abkommens innerhalb der nationalen Rechtsordnung,¹¹ ist einem solchen völkerrechtlichen Abkommen die Durchsetzungskraft gegenüber Gesetzen gewährleistet. Ein internationales Abkommen mit Ratifizierungsmöglichkeit für alle Staaten der Welt wäre m.E. im Interesse des Persönlichkeitsschutzes, eines freien Datenflusses und vor allem der Rechtssicherheit aller Beteiligten, ein erstrebenswertes Ziel.

Nicht erreicht ist diese Zielsetzung unter anderem dann, wenn ein solches Abkommen wichtige sachliche Probleme, wie z.B. die Frage der internationalen Datennetze, nicht lösen kann oder offen lässt. Der Zweck eines internationalen Abkommens muss darin liegen, alle sich dem nationalen Rechtskreis entziehenden, international noch ungeklärten Fragen auf supranationaler Ebene zu beantworten¹² und Unklarheiten zwischen den Staaten bezüglich Zuständigkeit, Rechtsanwen-

6 Ein internationales Abkommen das nicht nur einem bestimmten, innerhalb einer Organisation vertretenen Staatenkreis (z.B. OECD) offensteht, sondern auch afrikanischen, lateinamerikanischen und asiatischen Staaten einen Beitritt ermöglicht.

7 ORDEMANN, OeVD 6/77, S. 6; FREESE, Data Flow, S. 58.

8 Vgl. vorne, S. 23f.

9 Für den Datenverkehr zwischen Vertragsstaaten sollte im Normalfall keine Ausfuhrgenehmigung mehr erforderlich sein.

10 Vgl. vorne, S. 27ff., 39ff.

11 Uebersetzungsrang, Verfassungsrang oder Rang zwischen Verfassung und Gesetz.

dung und Verfahren eindeutig zu klären. Es wäre untragbar, die mit internationalen Datennetzen zusammenhängenden Fragen weiterhin ungeklärt zu lassen.¹³

Eine Abkommen vermöchte auch der Bildung von data havens entgegenzuwirken, indem es in einer Klausel den Austausch von personenbezogenen Daten eines Vertragsstaates mit Nichtmitgliedern auf die einmalige Ausfuhr von originären Daten beschränkt¹⁴ und damit einen geschlossenen Schutzkreis herstellt; innerhalb der Signatarstaaten aber müsste der Datenfluss frei zirkulieren können und jedem Mitglied die Pflicht zur Erhaltung eines freien Datenverkehrs mit allen Vertragsstaaten auferlegt werden.¹⁵ Eine derartige Regelung hätte eine repressive Wirkung (wenn auch nur in geringem Ausmass) auf die Nichtmitgliedstaaten, deren Einfluss im Interesse des Persönlichkeitsschutzes als positiv beurteilt werden kann. Die Ratifikation eines solchen Abkommens sollte im sozial- und wirtschaftspolitischen Interesse eines jeden Staates, dessen Wirtschaft und seiner Bürger liegen. In diesem Zusammenhang ist auch die weitsichtige Haltung einiger Datenschutzgesetzgeber hervorzuheben, die die Datenausfuhr von der Genehmigungspflicht ausgenommen haben, wenn eine internationale Vereinbarung Anwendung findet.¹⁶

-
- 12 Wie sind Daten geschützt, wenn sie in einem bestimmten Land gesammelt, in einem zweiten verarbeitet und in einem dritten gebraucht, kopiert und eventuell in allen drei Staaten veröffentlicht werden? Fragen dieser Art sind m.E. nur innerhalb eines internationalen Abkommens lösbar (vgl. auch CARMODY, Information Privacy, Vol. 1, No. 1, S. 27).
- 13 Vgl. Zitat EGER's: "If we are going to build global networks, we (=USA) can only do it with international agreements. We can't go around the rest of the world." (zit. PANTAGES/PIPE, S.123).
- 14 Vgl. vorne, S. 324ff.
- 15 Ähnlich STADLER, OeVD 1-2/79, S. 4; ferner in DS+DS 3/79, S. 170.
- 16 So im österreichischen (§ 32 Abs. 2 Ziff. 3 [vorne, S. 178]), dänischen (§ 21 Abs. 4, Gesetz für private Register [vorne, S. 204]) und norwegischen (§ 36 Abs. 3 [vorne, S. 210]) Datenschutzgesetz verwirklicht.

Es ist verständlich, dass die an einem internationalen Abkommen (z.B. Konvention) arbeitenden Organisationen bzw. Gremien, wie Europarat oder OECD, nicht alle Probleme des weltweiten Datenverkehrs berücksichtigen konnten und wollten. Die Lösung dieser Probleme auf einer globalen Ebene, zwischen den Staaten aller Kontinente, kann nur in dem von STADLER¹⁷ vorgeschlagenen Forum einer weltweiten Staatenkonferenz angegangen werden, die für Beratung und Beschlussfassung über eine "world order for the transborder flow of automated (and non automated)"¹⁸ datas" zuständig wäre.

Ein "internationales Rechtsregime"¹⁹ in Form einer weltumspannenden völkerrechtlichen Konvention als "Magna Charta" des Datenschutzes²⁰ ist somit das anzustrebende Endziel jeder Regelung des Persönlichkeitsschutzes im grenzüberschreitenden Datenverkehr.

II. Lösungskonzept: Internationales Rechtsregime zum Datenschutz

1. Form

Die Zielvorstellungen eines internationalen Rechtsregimes²¹ zur Regelung der grenzüberschreitenden Datenflüsse müsste z.B. in Form einer bindenden völkerrechtlichen Konvention verabschiedet werden, die auch Vorshriften materieller Natur enthalten sollte. Aus einer so konzipierten der Konvention könnten direkt Rechte abgeleitet werden, soweit das nationale Recht eines Mitgliedstaates zu bestimmten Punkten keine Vorschriften erlassen hat. Die Konvention sollte jedoch nicht das gesamte Spektrum des Datenschutzes abschliessend zu

17 STADLER, OeVD 1-2/79, S. 4.

18 In Klammern: Ergänzung des Verfassers, vgl. vorne, S. 349f.

19 STADLER, OeVD 1-2/79, S. 4; id., DS+DS 3/79, S. 170; FREESE, Data Flow, S. 8.

20 STADLER, DS+DS 3/79, S. 169f.; FREESE, a.a.O., S. 58.

21 Der Verfasser beschränkt sich darauf, ein Lösungskonzept mit einzelnen Beispielen vorzustellen, beabsichtigt aber nicht ein detailliert und abschliessend ausgearbeitetes Lösungsmodell vorzustellen.

regeln versuchen, sondern sich im wesentlichen auf die Aspekte des grenzüberschreitenden Datenverkehrs und die damit zusammenhängende Problematik konzentrieren, so dass dem nationalen Recht ein gewisser Raum für die eigenstaatliche Ausprägung von Datenschutzvorschriften offenbleibt.

Da eine Regelung des grenzüberschreitenden Datenverkehrs aber nicht von der nationalen Datenschutzgesetzgebung losgelöst werden kann, wird ein Konventionsrecht einen starken Einfluss auf die materielle und formelle Ausgestaltung eines nationalen Gesetzes haben. Diese Auswirkungen müssen nun vom nationalen Recht aufgefangen werden, damit die Regelung des transnationalen Verkehrs in den Kontext eines umfassenden Datenschutzes eingebettet werden kann und eine Anwendung des gleichen rechtlichen Instrumentariums für die nationale und internationale Stufe möglich wird.

2. Gründe und Argumente:

A. Für ein internationales Rechtsregime

Die Gründe, die für ein internationales Rechtsregime sprechen, ergeben sich teilweise aus den vorhergehenden Ausführungen in dieser Arbeit, teilweise werden sie hier ergänzend aufgeführt:

- Im System zum Schutz der Persönlichkeit können Lücken entstehen, weil die nationale Gesetzgebungs- und Rechtsprechungshoheit territorial beschränkt ist und nur vor Verletzungshandlungen innerhalb des eigenen Territoriums zu schützen vermag. Datenschutzgesetze können nicht effektiv und wirkungsvoll sein, wenn sie Raum lassen, die einzelnen nationalen Gesetze durch eine Verlagerung der Benutzeraktivitäten in eine andere Rechtsprechungshoheit zu umgehen bzw. durch exzessive Ueberlappungen diese Lücken zu schliessen versuchen. Mit einem internationalen Rechtsregime kann die Gefahr von Konflikten verschiedener nationaler Datenschutzgesetze und von Lücken zwischen national unterschiedlichen Datenschutzrechten vermieden werden.

- Zweck des Datenschutzes - national wie international - ist die Gewährleistung der Persönlichkeitsrechte und der damit verbundenen Grundfreiheiten. Diese Rechte sollen jedem Individuum, unbekümmert und ohne Unterschied von Nationalität und Wohnsitz zuerkannt werden.²²
- International koordinierte Regeln sind auch deshalb sinnvoll, weil die Computer-Technologie universell ist und in den verschiedenen Rechtssystemen zu ähnlichen Lösungen führen muss. Die Problemstellung des grenzüberschreitenden Datenverkehrs ist grundsätzlich überall die gleiche - ihre national unterschiedliche Regelung ist entweder das Resultat mangelnder Kooperation oder des unterschiedlichen Kontextes der nationalen Rechtsordnungen und Kulturen.
- Die Auseinandersetzung mit den gestellten Problemen erfolgt durch Spezialisten aus verschiedenen Ländern mit profunden Kenntnissen des Sachgebietes. Die Gewähr für eine ausgereifte Lösung ist grösser als beim Abschluss von zwischenstaatlichen Abkommen durch nationale Gremien, die oft nicht genügend die Schwierigkeiten und Komplexität des Themas zu erfassen vermögen und zu Lösungen kommen, welche zu Konflikten mit andern Bestimmungen und letzten Endes zu einem Kommunikationschaos führen können. (Ebenso gefährlich ist die Tatsache, dass infolge zu grosser Kompromisse bei internationalen Streitfragen Resultate mit nur schwacher Wirkung erzielt werden; diese drohen aber auch einer internationalen Konvention).
- Die Abwanderung der datenverarbeitenden Industrie in datenschutzfreie Gebiete wird eingeschränkt, wenn ein grosser Teil der Nationen in einer Konvention an die Beachtung der Datenschutzvorschriften gebunden ist und der Austausch mit Nichtmitgliedern einer Genehmigung bedarf. Die Attraktivität der Verlegung industrieller Tätigkeiten auf dem Gebiet der Datenverarbeitung in Nichtmitgliedstaaten wird verringert, weil überall vergleichbare Datenschutzbe-

22 HONDIUS, Information Privacy, Vol. 1, No. 1, S. 4.

stimmungen anwendbar sind und der Datenexport in Länder, welche der Konvention nicht angehören bzw. den Schutz der Persönlichkeit nicht genügend gewährleisten können, durch die Verweigerung einer Genehmigung gestoppt werden kann.

- Keiner der bestehenden internationalen Verträge²³ trägt den in verschiedenen Ländern existierenden Datenschutzgesetzgebungen Rechnung; dies unterstreicht die Notwendigkeit, Anstrengungen zur Schaffung internationaler Datenschutzbestimmungen in einem völkerrechtlichen Abkommen zu unternehmen. Aus der Kategorie der Verträge, welche die technischen Uebermittlungsmethoden²⁴ regeln und denjenigen zur Sicherung der internationalen Informationsfreiheit²⁵ ergeben sich Folgerungen für den grenzüberschreitenden Datenverkehr, die in einem internationalen Rechtsregime (z.B. Konvention) zu berücksichtigen wären. Ueberdies ist eine Konvention das geeignete Mittel, um für den internationalen Datenverkehr spezifische Bestimmungen und Ergänzungen zu erlassen, die Auswirkungen auf die genannten und andere völkerrechtliche Verträgen haben. Eine genaue Abgrenzung des Geltungsbereiches einer künftigen Konvention gegenüber bestehenden Verträgen ist notwendig, damit nicht bereits geklärte Punkte nochmals geregelt und Ueberschneidungen des Anwendungsbereiches vermieden werden können.²⁶
- Bedeutend ist der internationale wirtschaftliche Aspekt: Ein internationales Rechtsregime ermöglicht den multinationalen Gesellschaften eine Erleichterung ihrer internationalen Tätigkeit, eine Vereinfachung der zu beachtenden Regeln im grenzüberschreitenden Datenverkehr und grössere Rechtssicherheit in diesen datenverarbeitenden Aktivitäten.

23 Vgl. vorne, S. 27ff. und 39ff.

24 Internationaler Fernmeldevertrag, INTELSTAT-Abkommen, UNESCO-Deklarationen.

25 EMRK, UNO-Weltpakt, KSZE-Schlussakte.

26 MALLMANN, International agreements, S. 12, N 44.

- Neue Anwendungsformen der elektronischen Datenverarbeitung erwecken zusätzliche Bedürfnisse nach Datenschutz auf internationaler Ebene: "Electronic mail" wird als computerunterstützter Austausch von Informationen aller Art den internationalen Telex-, Telegramm- und Postverkehr, bis zu einem gewissen Grad ersetzen, insbesondere innerhalb multinationaler Gesellschaften. Beim Post-, Telegramm- und Telexverkehr sind die übermittelten Informationen durch das Brief- und Postgeheimnis der Länder geschützt, die der internationalen Postunion angeschlossen sind; beim "electronic mail" kann dieser Schutz ausfallen, weil die Informationen (dabei wird das Ineinanderfließen von Text- und Datenverarbeitung deutlich) über Telephonleitungen oder Satellitenverbindungen von einem Computer an ein anderes, im Ausland stehendes Datenverarbeitungssystem übermittelt werden. Ohne Datenschutz und Datensicherungs-normen auf internationaler Ebene kann ein gleichwertiger Ersatz für das bestehende Brief- und Fernmeldegeheimnis im internationalen Kommunikationsverkehr nicht geboten werden, es sei denn durch eine entsprechende Ergänzung des Fernmeldevertrages. Ein solcher Geheimnisschutz ist aber notwendig, um eine durch mangelnde rechtliche Sicherungen auf internationaler Ebene bewirkte Hemmung neuer Anwendungsbereiche der EDV zu vermeiden.

B. Gegen ein internationales Rechtsregime

Vereinzelte sind Gegenargumente und Skepsis zu hören, die aber weder die Gründe für eine Konvention zu überschatten noch deren Notwendigkeit in Frage zu stellen vermögen.

- PANTAGES/PIPE²⁷ glauben, dass zu viele Verträge, Gesetze, Bestimmungen und Meinungen gegenseitig und untereinander harmonisiert werden müssen, als dass eine wirkungsvolle Konvention erreicht würde.

27 PANTAGES/PIPE, S. 115ff.

- National unterschiedliche Interpretationen und Anwendungsformen der vereinbarten Normen können auch unter dem Regime einer internationalen Konvention zu einem Chaos führen.²⁸
- SAMET²⁹ bezweifelt die Effizienz einer internationalen Datenschutzregelung, weil eine Kontrolle oder Aufdeckung von Missbräuchen in der digitalisierten Uebermittlung nicht möglich sei: Um einen internationalen Datenschutz zu gewährleisten, müsse der internationale Datenfluss gestoppt oder zumindest einer Zensur und Kontrolle unterworfen werden.
- M.E. werden Probleme bei der Grenzziehung zwischen den allgemeinen Grundprinzipien bzw. Erfordernissen, die auf internationaler Ebene geregelt werden müssen, und Fragen, die der nationalen Ausgestaltung überlassen bleiben sollten, auftauchen.

Sollten alle Lösungsmöglichkeiten an einem Mangel an Bereitschaft zur internationalen Zusammenarbeit auf dem Gebiete des Datenschutzes scheitern, würde dies zur Verabschiedung einer Vielzahl von Gesetzen durch die vom grenzüberschreitenden Datenverkehr betroffenen Nationen führen und könnte in einem einzelstaatlichen Protektionismus, der Entstehung von "data havens" und einem durch nationale Schranken behinderten Informationsfluss enden.

3. Konzeption

Die nachfolgenden Vorschläge zur inhaltlichen Ausgestaltung eines internationalen Rechtsregimes gehen davon aus, dass eine vollständige Vereinheitlichung des Datenschutzrechts weder möglich noch erstrebenswert erscheint, weil dafür zu weitgehende Kompromisse für eine Einigung auf dem kleinsten gemeinsamen Nenner eingegangen werden müssten, deren Effekt letzten Endes zu einer Schwächung des Datenschutzes auf internationaler Ebene führen würde. Vielmehr sollen die nationalen Datenschutzgesetze mit ihrer spezifisch nationalstaatlichen Ausprägung auch innerhalb eines internationalen Rechtsregimes

28 PANTAGES/PIPE, a.a.O.

29 SAMET, Information Privacy, Vol. 1, No. 5, S. 231f.

anwendbar bleiben. Charakteristisch für das angestrebte Rechtsregime wäre jedoch, dass die nationalen Gesetze der Mitgliedstaaten bis zu einem gewissen Grad eine Vereinheitlichung bzw. Angleichung an die Grundprinzipien des Datenschutzes aufweisen würden. Nur für gewisse Aspekte, die nach einer einheitlichen Regelung des grenzüberschreitenden Datenverkehrs in allen Staaten rufen, würde die Konvention dieser Art materielle Normen rechtsetzender Natur aufstellen. Kollisionsnormen sollen das Datensubjekt bei der Orientierung über die Möglichkeit der Durchsetzung seiner individuellen Ansprüche innerhalb des geschlossenen Schutzgebietes unterstützen. Den notwendigen Beistand zur Realisierung seines Schutzes würde der Betroffene immer von seiner nationalen Behörde erhalten, die den Angelpunkt bei der Rechtsverwirklichung darstellt und dem Datensubjekt bei der Rechtsdurchsetzung auf internationaler Ebene Beistand leistet.

4. Inhalt ³⁰

A. Zielsetzung

Die Zielsetzung eines internationalen Rechtsregimes sollte mehrere Aspekte beinhalten und einen möglichst weiten Rahmen für eine globale Informationsordnung abstecken:

- Wahrung und Schutz der Persönlichkeitsrechte sowie des informati-
onellen Selbstbestimmungsrechts als Ausfluss der durch den Daten-
schutz garantierten Grundrechte beim Austausch personenbezogener
Daten über die Landesgrenzen hinweg (m.a.W. Ziel, den internatio-
nalen Datenverkehr unter Wahrung des Datenschutzes zu ermöglichen);
- die Beachtung des Prinzips der Informationsfreiheit und die damit
zusammenhängende Aufrechterhaltung eines freien transnationalen
Datenverkehrs unter den Mitgliedstaaten, der Voraussetzung jeder
wirtschaftlichen Entwicklung ist;
- die Schaffung eines Ausgleichs der gegensätzlichen Interessen von
Datenschutz und Informationsfreiheit;

30 Die Bestimmungen administrativer und formaler Natur wie z.B. Inkraftsetzung, Beitrittsmodus, Kündigung, Vorbehalte, Ergänzung etc. finden keine spezielle Erwähnung.

- die Vermeidung der Bildung von data havens i.S. von Territorien mit unvollständigem oder fehlendem Datenschutz ausserhalb und innerhalb ("Convention havens") des Konventionsgebietes;
- das Bekenntnis zur Freiheit der wirtschaftlichen, kulturellen und wissenschaftlichen Beziehungen ohne hemmende Schranken des nationalen Rechts unter Wahrung der Wettbewerbsneutralität des Datenschutzes.

Nebst diesen Hauptpunkten sind auch noch weitere Aspekte denkbar, wie z.B. die Sicherstellung der Verarbeitung personenbezogener Daten für Forschungs-, wissenschaftliche und statistische Zwecke unter erleichterten Bedingungen.

Eine solch umfassende Konvention entsprechend ihrer Zielsetzung, d.h. für die Schaffung eines internationalen Rechtsregimes, aufgebaut und gegliedert werden und in ihrer inhaltlichen Ausgestaltung³¹ zur Zielverwirklichung beitragen.

B. Allgemeine Bestimmungen

Die Ausgestaltung der allgemeinen Bestimmungen und Definitionen ist weitgehend vom Ausgangspunkt der angenommenen Grundprinzipien (noyau dur) abhängig. Aus ihm ergibt sich der Rahmen,³² der mit den Definitionen abgesteckt wird. Die Formulierung der Begriffe³³ folgt aus dem Kontext des Datenschutzes in seinen Bezügen auf datenverarbeitende Tätigkeiten.

Der Vorteil eines einheitlichen Definitionsspektrums wird bei den Anknüpfungsfragen im Kollisionsrecht³⁴ deutlich sowie beim

31 Während der vorangegangenen Ausführungen sind an verschiedenen Stellen explizite Vorschläge zur inhaltlichen Ausgestaltung eines internationalen Rechtsregimes gemacht worden, so dass es hier keiner Aufzählung der einzelnen Punkte mehr bedarf. Ich beschränke mich auf die Aufführung einzelner Beispiele, wo dies nicht erfolgt, ist ein Verweis auf die entsprechende Stelle zu finden.

32 Anwendungsbereich (i.w.S.), d.h. Anwendungsbereich i.e.S., Schutzbereich und sachlicher Geltungsbereich.

33 Wie z.B. verantwortliche Stelle, geschützter Personenkreis, Arten von Verarbeitungsvorgängen, Datenkategorien, Kontroll- und Rechtshilfebehörden.

34 Vgl. vorne, S. 314, Anm. 36 und S. 315.

Erlass bestimmter materieller Normen zum grenzüberschreitenden Datenverkehr.

Wichtig ist m.E., dass im Rahmen eines internationalen Rechtsregimes eine absolute Gleichbehandlung und Gleichstellung von In- und Ausländern nicht nur auf Vertragsebene, sondern auch in allen nationalen Datenschutzrechten und Verfahren zugrundegelegt wird.

C. Grundprinzipien des Datenschutzes

Ein sog. "noyau dur", wie er in der Europarats-Konvention³⁵ und in den OECD-Richtlinien³⁶ vorgesehen ist, bezweckt eine gewisse Vereinheitlichung der nationalen Datenschutzgesetze mit dem Ziel, dem Datensubjekt überall ungefähr die gleichen Rechte zu gewähren und dem Datenverarbeiter ähnliche Verpflichtungen aufzuerlegen, ohne Rücksicht darauf, in welchem Staat die Datenverarbeitung oder eine ihrer Phasen ausgeführt wird. Diese Grundprinzipien haben einen erheblichen Stellenwert, da sie den materiellen Rahmen der nationalen Datenschutzrechte bestimmen, in welchem der grenzüberschreitende Datenverkehr eingebettet wird und mit seinen spezifischen Bestimmungen daran anknüpft. Aber nicht allein für die rechtliche Ausgestaltung des grenzüberschreitenden Datenverkehrs sind solche Grundprinzipien von grosser Bedeutung, auch für die Lösung von Gesetzes- und Zuständigkeitskonflikten werden hier die Voraussetzungen³⁷ geschaffen.

Bezüglich der inhaltlichen Konzeption eines noyau dur ist an erster Stelle das Postulat nach einem möglichst weiten Anwendungsreich aufzustellen. Damit soll nicht ein möglichst weiter Schutzzumfang angestrebt, sondern zugleich Inkompatibilitäten, die beim grenz-

35 Vgl. vorne, S. 250ff.

36 Vgl. vorne, S. 274ff.

37 Z.B. die Identifizierbarkeit einer verantwortlichen Stelle. Im noyau dur ist beispielsweise eine Vorschrift denkbar, die für jede Datensammlung bzw. -verarbeitende Stelle die Bezeichnung eines verantwortlichen Organs vorschreibt, d.h. die Bestimmung der verantwortlichen Stelle erfolgt durch einen normativen Akt, nicht aufgrund bestimmter Eigenschaften.

überschreitenden Datenverkehr³⁸ und bei der Lösung von Kollisionsproblemen³⁹ auftreten können, vorgebeugt werden.

Der Vorbehalt einer Einschränkung des Anwendungsbereiches (i.w.S.) für bestimmte Aspekte⁴⁰ wird trotzdem unumgänglich sein. Dabei ist m.E. die präjudizierende Wirkung eines weiten Rahmens auf die nationalen Datenschutzgesetze nicht zu unterschätzen, vor allem weil aufgrund einer derartigen weiten Konzeption die Möglichkeiten eines umfassenden Schutzes konkret sichtbar werden. Dieser Einfluss wird vor allem in jenen Ländern zum Tragen kommen, die noch kein Datenschutzgesetz erlassen haben, aber auch in Nationen, die bereits in der Phase des Erlassens oder der Novellierung von Datenschutznormen stehen, und darin seinen Ausdruck finden, dass die nationalen Gesetze vermehrt auf die internationale Dimension ausgerichtet werden, als Folge einer im Rechtsregime erkennbaren internationalen Informationsordnung und Informationspolitik.

Im weiteren haben die Grundprinzipien die materiellen Voraussetzungen dafür zu schaffen, dass eine Geltendmachung der Individualrechte im internationalen Rahmen überhaupt möglich wird, z.B. durch Informationen über Datenbestände und Datenflüsse im internationalen Verkehr,⁴² und sie dabei einen ausreichenden, nicht bloss minimalen Schutz gewährleisten.⁴³

38 Z.B. manuelle und automatisierte Verarbeitung.

39 Z.B. negative Auswirkungen für Datensubjekte aufgrund der Anknüpfung, die u.U. nur zu einem unbefriedigenden Resultat bei national unterschiedlichem Schutz von manuell und automatisiert verarbeiteten Daten führen kann.

40 Z.B. - Schutzbereich: Beschränkung auf natürliche Personen;
- Geltungsbereich: nur für automatisiert verarbeitete Daten.

41 Gl.M. Kirby, 12 Law and computer technology 3 (1979), S. 61.

42 U.U. kann in einigen Fällen darauf verzichtet werden, wenn sich dies aus dem Zweck und Grund der Informationserteilung bereits ergibt (z.B. Banküberweisung, Flugreservation).

43 Z.B. Beachtung der Zweckverwendung der Daten in allen Importländern bzw. keine Aenderung des Verarbeitungszweckes gegenüber demjenigen des Ursprungsstaates (Zweckverwendung ist schon bei Sammlung und Erhebung der Daten von Bedeutung).

Wichtig erscheint mir, dass das internationale Rechtsregime seine Grundprinzipien für den öffentlichen und privaten Bereich in differenzierter Form konzipiert, da eine Gleichbehandlung eine kontraproduktive Wirkung haben kann⁴⁴ und ein effizienter Datenschutz differenzierte Lösungen voraussetzt.

D. Bestimmungen zum grenzüberschreitenden Datenverkehr

Die Bestimmungen zum grenzüberschreitenden Datenverkehr müssen auf dem vom noyau dur geschaffenen Fundament eines gleichwertigen Schutzes der Daten in allen Mitgliedsländern aufbauen können und einen freien grenzüberschreitenden Datenfluss unter den Signatarstaaten sicherstellen.

Dieser Teil einer Konvention enthält die zentralen Vorschriften für ein internationales Rechtsregime zur Regelung des grenzüberschreitenden Datenverkehrs und trägt hauptsächlich zur Realisierung der in der Zielsetzung⁴⁵ niedergelegte Grundsätze bei. Dabei wird evident, dass dieses Ziel nicht alleine mit der Anerkennung von Grundprinzipien⁴⁶ erreicht werden kann, denn dort, wo eine einheitliche Lösung bestimmter Problemkreise⁴⁷ notwendig ist (weil auf nationaler Stufe nur ein unbefriedigendes Resultat erzielt werden kann), müssen materiell rechtsetzende Normen zur Anwendung kommen. Diese ein Einheitrecht bildenden Normen haben unmittelbare Auswirkungen auf nationaler Ebene, indem die aus ihnen fließenden Ansprüche direkt geltend gemacht werden können und keiner vorgängigen Umsetzung in das nationale Recht bedürfen; ausserdem gehen sie aufgrund ihrer höherrangigen Einstufung⁴⁸ dem anderslautenden oder widersprechenden nationalen Recht vor.

44 Vgl. vorne, S. 251ff.

45 Vgl. vorne, S. 250ff.

46 Z.B. Prinzip der Weiterleitungspflicht von Korrekturen, Ergänzungen, Löschung übermittelter Daten.

47 Z.B. Wiederexportes von Daten aus Konventionsgebiet an Drittstaaten: Frage der Wiederexportberechtigung (vgl. vorne, Lösungsmodell, S. 324).

48 Vgl. vorne, S. 392, Anm. 11.

Mit dieser Konzeption ist m.E. der durch die Zielsetzung abgesteckte Rahmen von Prinzipien zur Regelung des grenzüberschreitenden Datenverkehrs realisierbar. Die Bestimmungen über den grenzüberschreitenden Datenverkehr können demgemäss Aussagen über folgende Fragen enthalten:⁴⁹

- wie zwischen den Mitgliedstaaten der Grundsatz des freien⁵⁰ Flusses personenbezogener Informationen verwirklicht wird;
- in welchen Fällen eine Durchbrechung des Grundsatzes, d.h. eine Einschränkung des Datenflusses durch einen Mitgliedstaat⁵¹ zulässig ist;
- unter welchen Voraussetzungen ein Datenverarbeiter sich auf das Recht zur genehmigungsfreien Ausfuhr bzw. Einfuhr von Daten gemäss einer derartigen Konvention berufen kann,⁵² wenn ein Mitgliedstaat dem freien Datenverkehr ungerechtfertigterweise künstliche Schranken und Hindernisse entgegenstellt;
- dass jeder Vertragsstaat hinsichtlich seiner Uebermittlungsträger und Telekommunikationsmedien sicherstellen muss, dass sowohl ein ununterbrochener Transitverkehr als auch Import- und Export von Daten gewährleistet ist;
- wie die Transparenz im grenzüberschreitenden Datenverkehr verwirklicht wird und welche formellen Voraussetzungen dafür durch die verantwortlichen Stellen vor einer Ausfuhr und während der Verarbeitung im Ausland erfüllt werden müssen;⁵³
- welche erhöhten Datensicherungsvorkehrungen beim grenzüberschreitenden Datenverkehr als präventive Massnahmen durch die verantwortlichen Stellen beachtet und angewandt werden müssen;^{54 55}

49 Keine abschliessende Aufzählung.

50 D.h. genehmigungsfreier Export und Import.

51 Z.B. bei Gefährdung der nationalen Sicherheit.

52 Aufsichtsinstanz kann entweder entscheidende Befugnis haben, oder nur beratende Funktion hinsichtlich der Ausübung und Implementierung dieser Konvention besitzen.

53 Z.B. Eintrag im Datenregister und Vermerk in einem "Datenindosament", Nachweis der Datensicherungsvorkehrungen.

54 Vgl. vorne, S. 379.

55 Z.B. HW- und SW-mässige Verschlüsselung, Datengeheimnis.

- unter welchen Bedingungen ein Export gegenüber Mitgliedstaaten erfolgen kann, welche für ihr Gebiet eine Einschränkung des Anwendungsbereiches beschlossen haben;⁵⁶
- mit welchem Grundsatz verhindert werden soll, dass Daten aus Konventionsgebiet in Drittstaaten gelangen, welche keine ohne oder nur mangelhafte Datenschutzvorschriften entwickelt haben;⁵⁷
- welche Massnahmen gegenüber einem Mitgliedstaat vorgesehen sind, der keinen ausreichenden Datenschutz gewährleistet und in dem wiederholt Persönlichkeitsverletzungen erfolgt sind, welche die Zielsetzung der Konvention gefährden;⁵⁸
- mit welchen Massnahmen die Beachtung der in der Konvention enthaltenen Prinzipien und Normen durchgesetzt werden kann;⁵⁹
- wie die zweckgebundene Verarbeitung, dort wo sie im privaten Bereich normiert ist, auch im Ausland sichergestellt wird;⁶⁰
- welche Pflichten den verantwortlichen Stellen auferlegt werden müssen, damit die Datenqualität übermittelter Daten im Konventionsgebiet gewährleistet ist;⁶¹

56 Z.B. durch Gleichstellung mit einem Drittstaat, der für das betreffende Datensubjekt (z.B. juristische Person) keinen Schutz kennt und vorsieht.

57 Z.B. durch exklusive Befugnis des Ursprungsstaates zum Export von originären Daten (vgl. vorne, S. 324ff.). Mit einer solchen Regelung sind die nationalen Interessen, die bei einem Export in Nichtmitgliedstaaten tangiert werden können, am besten gewährt: Jeder nationalen Genehmigungsbehörde steht es frei die Ausfuhr der originären Daten in ein Nichtmitgliedsland zu gestatten, wenn daraus keine Gefährdung resultiert. Diese Lösungsvariante verhindert, dass im Ursprungsland nicht erhältliche Daten in einem anderen Mitgliedstaat verfügbar gemacht werden können und damit Entscheidungen des nationalen Gesetzgebers umgangen werden. (Es lassen sich auch Kompetenzstreitigkeiten vermeiden, die bei einer Rückfragepflicht des Mitgliedstaates beim Ursprungsland entstehen könnten.)

58 Z.B. Isolation durch Genehmigungssysteme, Ausschluss aus Mitgliedschaft.

59 Z.B. Ueberprüfung durch nationale Datenschutzbehörde (sollte in noyau dur postuliert worden sein).

60 Z.B. durch standardisierten Zwecknachweis.

61 Z.B. Weiterleitungspflicht angezeigter/verfügter Korrekturen, Ergänzungen, Löschungen etc., vgl. vorne, S. 378.

- wie unter Mitgliedstaaten, die trotz Rechtsangleichung durch die Grundprinzipien noch nationale abweichende Regelungen haben, vermieden wird, dass der freie Export und Wiederimport dazu benützt werden kann, die Schutzvorschriften in dem Staat zu umgehen, aus dem die Daten exportiert werden⁶² (auch eine Nutzung der Daten aus ausländischen Datenbanken, deren Verarbeitung im Benutzungsland untersagt ist, fällt unter diese Bestimmung);
- wie der Transitverkehr durch Mitgliedstaaten sichergestellt ist und störungsfrei erfolgen kann (d.h. welche Vorkehrungen vom nationalen Gesetzgeber für einen störungsfreien Verkehr getroffen werden müssen).

Die Vielfalt der verschiedenen Arten von Regelungstatbeständen rechtfertigt m.E. die Redaktion dieses Teils in einer Konvention in Form von Prinzipien und materiellen Vorschriften.

E. Kollisionsnormen⁶³

Innerhalb eines Konventionsgebietes, das einen Schutzraum für personenbezogene Daten darstellt und unter seinen Mitgliedstaaten den freien Informationsfluss gewährleistet, müssen Bestimmungen vorhanden sein, die darüber Auskunft geben, welches nationale Recht bei einer Persönlichkeitsverletzung zur Anwendung kommt, das als Folge eines sich über mehrere Vertragsstaaten erstreckenden Verarbeitungsvorganges eintritt. Aber nicht nur im Verhältnis der Mitgliedstaaten untereinander muss eine Bestimmung der Zuständigkeit und des anwendbaren Rechts erfolgen, es ist auch eine Vorschrift für die Beziehung der Konventionsstaaten zu Drittstaaten notwendig, welche die aus solchen Beziehungen resultierenden Auswirkungen auf die andern Mitgliedstaaten der Konvention normiert.

62 Z.B. durch Prinzip des Exportverbotes zu Umgehungszwecken in andern Mitgliedstaaten mit entsprechenden Massnahmen und Sanktionen (Durchbrechung des Grundsatzes des freien Exportes und Importes).

63 Vgl. ausführliche Analyse dieses Problemkreises in § 12, vorne, S. 300ff.

Wie bereits angeführt ⁶⁴ wurde, ist die Lösung des Kollisionsproblems, d.h. die Bestimmung der Anknüpfungspunkte bei Kollisionsnormen, vom Kontext des nationalen Datenschutzrechtes abhängig. Im Rahmen eines internationalen Rechtsregimes bedeutet dies, dass sich sowohl aus dem noyau dur, den Bestimmungen zum grenzüberschreitenden Datenverkehr, wie auch aus den Vorschriften zur Rechtshilfe auf internationaler Ebene die Notwendigkeit für eine einheitliche Anknüpfung unter den Mitgliedstaaten ableiten lässt. Wegen dieser Interdependenz der einzelnen Bereiche darf m.E. das Anknüpfungproblem nicht gesondert behandelt ⁶⁵ werden. Die mit der Anknüpfung verbundenen Probleme müssen ihren Ausdruck auch in den übrigen Prinzipien und Bestimmungen einer internationalen Konvention finden.

Die Wirksamkeit der Verhinderung von data havens, die durch ein "Convention gap" ("Ausflussrohr unter den Mitgliedstaaten") entstehen können, ist u.a. von der Konzeption des Kollisionsrechtes ⁶⁶ der Mitgliedstaaten gegenüber Drittländern abhängig.

Kollisionsnormen sind in einem Rechtsregime insofern unerlässlich, als sie die fundamentalen Bestimmungen zum Schutz bzw. Verwirklichung der aus dem Datenschutz fliessenden Rechte enthalten. Aus ihnen muss das im Konventionsgebiet befindliche Datensubjekt ersehen können, wo es seine Ansprüche geltend machen kann und welches Recht bei streitigen und nichtstreitigen Ansprüchen zur Anwendung kommt.

Auch hier könnte sich als Lösungsformel für eine Anknüpfung die Unterscheidung nach Individualrechten, die in nichtstreitigen Verfahren ⁶⁷ und solchen, die in streitigen Verfahren ⁶⁸ geltend gemacht werden, als praktikabel erweisen.

Aber nicht nur hinsichtlich des privaten Sektors ist Zuständigkeit und anwendbares Recht zu bestimmen, eine Klärung der Rechtslage hat auch für den öffentlichen Bereich zu erfolgen.

64 Vgl. vorne, S. 386ff.

65 Vgl. Rapport explicatif, N. 23

66 Z.B. durch Verlagerung des Kollisionsproblems von Konventionsstufe auf nationale Stufe gemäss dem Ursprungsprinzip; vgl. vorne, S. 324ff.

67 Vgl. Ausführungen und Begründung, vorne, S. 387.

68 Vgl. Ausführungen und Begründung, vorne, S. 388.

In diesem Teil sollten im weiteren auch Vorschriften existieren, die für das Konventionsgebiet das anwendbare Recht im Fall eines Eingriffs in Transitdatenflüsse sowie bei einer Beeinträchtigung der Persönlichkeitsrechte infolge störender Einwirkungen bei Uebermittlungen durch Satelliten bestimmen.

Bei der Verwirklichung des Schutzes der Persönlichkeitsrechte, des freien Datenflusses und der Vermeidung von data havens als schutzlose Räume ausserhalb und innerhalb des Konventionsgebietes kommt den Kollisionsnormen eine entscheidende Stellung zu, vor allem weil sie die Lösung für die Durchsetzung der Ansprüche aus dem Individualschutz durch die Bestimmung des anwendbaren Rechts und der Zuständigkeit im internationalen Rahmen beinhalten.

F. Rechtshilfe und Zusammenarbeit der Behörden

Die Rechtshilfe verkörpert die vierte tragende Säule zur Erreichung der projektierten Ziele: Die Durchsetzung der aus dem Datenschutz den Betroffenen als auch den verantwortlichen Stellen übertragenen Rechte und Pflichten wird auf internationaler Ebene scheitern, wenn die Rechtshilfe und internationale Zusammenarbeit nicht reibungslos funktioniert.

Wichtig ist, dass die Rechtshilfe sowohl im privaten wie im öffentlichen Bereich direkt zwischen den zuständigen nationalen Behörden abgewickelt werden kann. Im öffentlichen Sektor können allerdings, verursacht durch Souveränitätsfragen, Probleme auftauchen, die eine direkte Zusammenarbeit erschweren, so dass hier die Wahrnehmung der Rechte und der internationale Verkehr unter den Datenschutzbehörden nur eingeschränkt vollzogen werden kann.

Ein internationales Rechtsregime muss die rechtlichen Grundlagen für eine enge wirksame Zusammenarbeit der nationalen Datenschutzbehörden schaffen. Es kann sich dabei auf die traditionellen Prinzipien und Methoden abstützen, mit denen bereits auf anderen Rechtsgebieten eine erfolgreiche Zusammenarbeit erreicht wurde und weiterhin fortgeführt wird.⁶⁹

69 Z.B. internationale Rechtshilfeabkommen in Zivil- und Strafsachen.

Die Konzeption der Rechtshilfe basiert dabei auf den nationalen Datenschutzbehörden; die Errichtung einer internationale Superbehörde erscheint mir wenig zweckmässig, da die Rechtshilfe möglichst nah beim Datensubjekt lokalisiert sein muss. Eine internationale Behörde könnte als Konsultativ-, Ueberwachungs- und gegebenenfalls als Vermittlungsorgan sinnvoll tätig werden, hingegen nicht als Entscheidungsbehörde. Dem Schutzzweck des Datenschutzes wird durch die Inanspruchnahme der für den Datenverarbeiter bzw. den Betroffenen zuständigen nationalen Instanzen am besten entsprochen. Ein gutes Zusammenwirken der nationalen Behörden erübrigt eine internationale Ueberwachungsbehörde.⁷⁰ In seiner inhaltlichen Ausgestaltung ist in der KE⁷¹ bedeutende Vorarbeit geleistet worden. Die Rechtshilfe sollte für alle Phasen des internationalen Datenverkehrs ausgebaut werden, d.h. sowohl in der Orientierungsphase,⁷² in der Untersuchungsphase wie auch bei der Geltendmachung von Ansprüchen. Zur Rechtshilfe gehört aber auch die Weiterleitung von Urteilen, Verfügungen, Massnahmen und Rechtsbegehren. Schliesslich sollte die Konvention auch konkrete Normen enthalten, welche die Durchsetzung der Rechte des Betroffenen auf internationaler Ebene gewährleisten. Auf jeden Fall müssen Sicherungsvorkehrungen eingebaut werden, die einen Missbrauch der Zusammenarbeits- und Rechtshilfemechanismen verhindern.

Für die aus der Rechtshilfe anfallenden Kosten müssen die Mitgliedstaaten eine sozial angemessene Lösung entwickeln. Allerdings können die Lasten der Rechtshilfe in erträglichen Grenzen gehalten werden, wenn eine internationale Konvention verabschiedet wird, die einen umfassenden wirkungsvollen Schutz der Persönlichkeit gewährleistet - die Interdependenz ist offensichtlich.

70 BENJAMIN, Online, S. 7.

71 Vgl. vorne, S. 261ff.

72 Auskunft über Erfüllung der Voraussetzungen zum Export (Registereintrag), Auskunft über Destination des Exportes falls Deklarationspflicht statuiert ist.

G. Spezialbestimmungen

Aufgrund des breiten Spektrums der Erscheinungsformen des grenzüberschreitenden Datenverkehrs sollte in einem internationalen Rechtsregime auch Raum für Spezialerlasse und Ergänzungsvereinbarungen vorgesehen werden. Solche präzisierende Bestimmungen können sich wegen des speziellen Charakters der personenbezogenen Informationsverarbeitung gegenüber bestehenden, den allgemeinen Informationsverkehr betreffenden völkerrechtlichen Verträgen u.U. als notwendig erweisen.

Als Spezialbestimmungen sind z.B. spezielle Normen zur Regelung des Datenverkehrs von internationalen Organisationen denkbar, die aufgrund ihres besonderen Status und ihres Tätigkeitsfeldes Spezialvorschriften erfordern können.⁷³ Ferner sind bereichsspezifische Regelungen für Daten bestimmter Kategorien denkbar, wie z.B. medizinische, statistische, wissenschaftliche und Forschungsdaten.

Präzisierende Bestimmungen über den personenbezogenen Informationsverkehr sind u.U. in Ergänzung von bestehenden internationalen Abkommen,⁷⁴ die die Telekommunikation zum Regulationsgegenstand haben, angebracht. So sind z.B. Vorschriften für die Uebermittlung von Daten durch Satelliten denkbar, welche die Berücksichtigung der spezifischen Aspekte des Datenschutzes im Weltraum, d.h. ausserhalb der Grenzen des nationalen souveränen Territoriums und des Luftraumes der Konventionsstaaten, regeln.⁷⁵

73 Z.B. INTERPOL, WHO, FAO, UNESCO, UNO, u.U. NATO mit NICS-Netz.

74 Z.B. - UNESCO, Declaration of Guiding Principles on the Use of Satellite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange, General Conference 1972.

- Internationaler Fernmeldevertrag von Malaga-Torremolinos, 1973.

75 GOTLIEB/DALFEN/KATZ S. 236.

III. Schlussfolgerung

Abschliessend soll die zusammenfassende Sicht eines der bedeutendsten Experten im Themenkreis des grenzüberschreitenden Datenverkehrs die vorangegangenen Betrachtungen nochmals erhärten: "Die Entwicklung der nationalen Datenschutzgesetze, die zunehmende Bedeutung des grenzüberschreitenden Datenverkehrs und der Aufbau internationaler Informationsnetze führen zu Schwierigkeiten für die internationale Datenverarbeitung bei unterschiedlichen Regelungen in den verschiedenen Staaten und durch die einzuholenden Bewilligungen, bringen aber auch für die durch den Datenschutz zu schützenden Personen Probleme, da Lücken in den Datenschutzbestimmungen ausgenützt werden können, der Betroffene seine Rechte auf Einsicht usf. im Ausland verfolgen muss u.ä. Die Bemühungen um eine internationale Koordination der nationalen Datenschutzrechte sind daher dringlich, soll nicht der internationale Informationsverkehr und damit die internationale Wirtschaft empfindlich gestört werden."⁷⁶

Der in die Form eines Paradoxons gekleideten Aussage JAN FREESE's ⁷⁷ ist deshalb zuzustimmen, wenn er folgert: "The free and balanced international data flow must be regulated in order to remain balanced and free".

⁷⁶ STADLER, OeVD 12/79, S. 3.

⁷⁷ FREESE, Data Flow, S. 70.

Curriculum vitae

Am 29. Januar 1950 wurde ich in Zürich geboren und wuchs hier bis zum vierten Lebensjahr auf. Danach verbrachte ich meine Jugend in Thalwil, wo ich vom Frühjahr 1957 bis zum Frühjahr 1963 die Primarschule besuchte. Im Anschluss daran absolvierte ich die ersten drei Gymnasialjahre an der Kantonsschule Freudenberg in Zürich; die restlichen fünf Gymnasialklassen durchlief ich in der Stiftsschule des Klosters Einsiedeln, an der ich im Juli 1971 die Matura Typus A bestand. Im Wintersemester 1971/72 immatrikulierte ich mich an der Medizinischen Fakultät der Universität Zürich; nach drei Semestern wechselte ich im Frühjahr 1973 an die Rechts- und staatswissenschaftliche Fakultät. Im Dezember 1977 wurde ich zum lic. iur. promoviert. Gleichzeitig mit dem Beginn der Doktorarbeit, im Januar 1978, nahm ich meine während des Studiums begonnene Tätigkeit als Werkstudent bei einer Computerfirma, die ich für die Dauer der Lizentiatsprüfungen unterbrochen hatte, wieder auf, um meine EDV-Kenntnisse auch im Hinblick auf die Doktorarbeit zu erweitern. Diese Halbtagsstellung beendete ich mit Abschluss meiner Dissertation im August 1980. Am 1. September 1980 trat ich zur praktischen juristischen Ausbildung das Auditorenjahr am Bezirksgericht Zürich an. Am 27. Mai 1981 erfolgte die Promotion zum Doktor der Rechtswissenschaft.

